Alarm Guide for the Cisco Mobile Wireless Transport Manager 6.1.7

March 12, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25465-01

Alarm Guide for the Cisco Mobile Wireless Transport Manager 6.1.7

MWTM ALARM GUIDE

4.5 EntityConfiguration
4.6 RMONRising
4.7 RMONFalling
4.8 FlashDevice
4.9 ModuleStatus
4.10 PowerStatus
4.11 IPSLAReaction
4.12 IPSLAGroupStatus
4.13 IPSLATimeout
4.14 IPSLAOverThreshold
4.15 IPSLADataCorruption
4.16 IPSLADiscoveryFailed
4.17 IPSLAConnectionLost
4.18 RebootDetected
4.19 InterfaceState
4.20 SlbVirtualServerStateChange
4.21 SlbRealServerStateChange
4.22 SlbFaultToleranceStateChange
4.23 ModuleStatusState
4.24 LOS
4.25 LOF
4.26 RAI
4.27 AIS
4.28 ShutdownAlarm
4.29 SupplyStateChange
4.30 FanStateChange
4.31 DS1LineStatusRcvFarEndLOF
4.32 DS1LineStatusXmtFarEndLOF
4.33 DS1LineStatusRcvAIS
4.34 DS1LineStatusXmtAIS
4.35 DS1LineStatusLOF
4.36 DS1LineStatusLOS
4.37 DS1LineStatusLoopback
4.38 DS1LineStatusT16AIS
4.39 DS1LineStatusRcvFarEndLOMF
4.40 DS1LineStatusXmtFarEndLOMF
4.41 DS1LineStatusRcvTestCode
4.42 DS1LineStatusOtherFailure
4.43 DS1LineStatusUnavailSigState
4.44 DS1LineStatusNetEquipOOS
4.45 DS1LineStatusRcvPayloadAIS
4.46 DS1LineStatusPerfThreshold
4.47 NodeTimeZoneChange
4.48 NodeUnreachable
4.49 TrapRateStatus
4.50 FailoverDetected
4.51 SnmpError
4.52 ConfigurationDownload
4.53 MemoryBufferElementsFree
4.54 FreeMemory
4.55 ChassisPowerSupply1
4.56 ChassisPowerSupply2
4.57 CpmCPUavgBusy5
4.58 ChassisTempAlarm
4.59 ChassisMajorAlarm
4.60 ChassisMinorAlarm
4.61 MWTMDatabaseError
4.62 MWTMDiskUtilization
4.63 MWTMCriticalAlarm
4.64 MWTMMajorAlarm
4.65 MWTMMinorAlarm
4.66 MWTMWarningAlarm
4.67 MWTMInformationalAlarm
4.68 MWTMNormalAlarm
4.69 RedundancyState
4.70 SystemFreeMemory
4.71 EnhancedFreeMemoryState
4.72 FreeMemoryState
4.73 UnknownTrap
4.74 NsoActive
4.75 NsoState

4.76 CPUThreshold
4.77 HistoryEventConfigDestination
4.78 ConfigManEvent
4.79 CLIRunningConfigChanged
4.80 HSRPState
4.81 FlashCopyCompletion
4.82 FlashPartitioningCompletion
4.83 FlashMiscOpCompletion
4.84 FRU
4.85 SyslogEvent
4.86 AuthenticationFailure
4.87 ChassisAlarm
4.88 MemBufferNotify
4.89 Loopback
4.90 EEM-ServerEvent
4.91 EEM-PolicyEvent
4.92 TcpConnectionClose
4.93 CefInconsitencyState
4.94 CefPeerFIBState
4.95 CefPeerState
4.96 ExpFwdResourceFailure
4.97 EntityAlarmAsserted
4.98 Syslog
4.99 NodeState
4.100 SnmpTimeout
4.101 ApplicationError
4.102 GroupState
4.103 NodeIgnoredSet
4.104 RtrInterfaceIgnoredSet
4.105 NodeProcessTrapsSet
4.106 ObjectModelPurged
4.107 NodeUserDataUpdated
4.108 RtrInterfaceUserDataUpdated
4.109 NodeManagementUpdated
4.110 DiscoveryRequested
4.111 PollRequested
4.112 NodeDeleted
4.113 RtrInterfaceDeleted
4.114 FileModification
4.115 Login
4.116 Logout
4.117 ProvisionRequest
4.118 LaunchTerminal
4.119 GroupIgnoredSet
4.120 GroupUserDataUpdated
4.121 GroupDeleted

Section **5 GGSN**

5.1 APN-ConfigModified
5.2 APN-UpstreamSecurityViolation
5.3 APN-DownstreamSecurityViolation
5.4 APN-ServiceMode
5.5 ChargingGatewayMaintenanceMode
5.6 ChargingGatewayState
5.7 ChargingGatewaySwitchover
5.8 GTPPathFailed
5.9 DCCARatingFail
5.10 DCCAServiceDenied
5.11 CSGState
5.12 DCCACreditLimitReached
5.13 DCCAUserUnknown
5.14 DCCAAuthReject
5.15 GWServiceState
5.16 APN-NoResources
5.17 GWMaintenanceMode
5.18 APN-NoRadius
5.19 GWMemoryThreshold
5.20 PSDDiskFull
5.21 PSDServerState
5.22 APN-IpAllocationFail

SECTION 1.1

Status: BWGBaseStationsThreshold

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BWGBaseStationsThreshold	Poll	Alarm	Yes	Critical	$NodeDisplayName - Current number of base stations on BWG ($cagwInstanceDescription): $cagwCurrentBaseStations. Maximum Allowed: $cagwMaximumBaseStations. Utilization $BWGBaseStationsUtilizationPercent%.	BWGBaseStationsThreshold	BWG
BWGBaseStationsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - Current number of base stations on BWG ($cagwInstanceDescription): $cagwCurrentBaseStations. Maximum Allowed: $cagwMaximumBaseStations. Utilization $BWGBaseStationsUtilizationPercent%.	BWGBaseStationsThreshold	BWG
BWGBaseStationsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - Current number of base stations on BWG ($cagwInstanceDescription): $cagwCurrentBaseStations. Maximum Allowed: $cagwMaximumBaseStations. Utilization $BWGBaseStationsUtilizationPercent%.	BWGBaseStationsThreshold	BWG
BWGBaseStationsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - Current number of base stations on BWG ($cagwInstanceDescription): $cagwCurrentBaseStations. Maximum Allowed: $cagwMaximumBaseStations. Utilization $BWGBaseStationsUtilizationPercent%.	BWGBaseStationsThreshold	BWG

Description:

This status alarm is generated whenthe ratio of base stations (cagwCurrentSubscribers) relative to the maximum allowed (cagwMaximumBaseStations) causes BWGBaseStationsThreshold to transition between the Critical, Major, Warning, and Normal states.

Default Message:

- $NodeDisplayName - Current number of base stations on BWG ($cagwInstanceDescription): $cagwCurrentBaseStations. Maximum Allowed: $cagwMaximumBaseStations . Utilization $BWGBaseStationsUtilizationPercent%.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
BWGBaseStationsThreshold	Indicates the utilization of the BWG Gateway. - Critical: 100% utilized. The maximum number of base stations that can be concurrently supported by this BWG has been reached. - Major: Between 90% to 100% utilized [90%-100%). - Warning: Between 80% to 90% utilized [80%-90%). - Normal: Less than 80% utilized [0%-80%).
cagwCurrentBaseStations	The number of subscribers currently connected to this BWG.
cagwMaximumBaseStations	The maximum number of base stations that can be concurrently supported by this BWG.
BWGBaseStationsUtilizationPercent	The ratio of cagwCurrentBaseStations / cagwMaximumBaseStations expressed as a percent.
cagwInstanceDescription	Description of the physical instance of the BWG.
cagwInstanceIndex	An index that uniquely represents each BWG Gateway per device. This index is assigned arbitrarily by the engine and is not saved over reboots.

Operational Information:

Go Top

SECTION 1.2

Status: BWGSubscribersThreshold

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BWGSubscribersThreshold	Poll	Alarm	Yes	Critical	$NodeDisplayName - Current number of subscribers on BWG ($cagwInstanceDescription): $cagwCurrentSubscribers . Maximum Allowed: $cagwMaximumSubscribers . Utilization $BWGSubscribersUtilizationPercent%.	BWGSubscribersThreshold	BWG
BWGSubscribersThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - Current number of subscribers on BWG ($cagwInstanceDescription): $cagwCurrentSubscribers . Maximum Allowed: $cagwMaximumSubscribers . Utilization $BWGSubscribersUtilizationPercent%.	BWGSubscribersThreshold	BWG
BWGSubscribersThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - Current number of subscribers on BWG ($cagwInstanceDescription): $cagwCurrentSubscribers . Maximum Allowed: $cagwMaximumSubscribers . Utilization $BWGSubscribersUtilizationPercent%.	BWGSubscribersThreshold	BWG
BWGSubscribersThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - Current number of subscribers on BWG ($cagwInstanceDescription): $cagwCurrentSubscribers . Maximum Allowed: $cagwMaximumSubscribers . Utilization	BWGSubscribersThreshold	BWG

					$BWGSubscribersUtilizationPercent%.		

Description:

This status alarm is generated whenthe ratio of subscribers (cagwCurrentSubscribers) relative to the maximum allowed (cagwMaximumSubscribers) causes BWGSubscribersThreshold to transition between the Critical, Major, Warning, and Normal states.

Default Message:

- $NodeDisplayName - Current number of subscribers on BWG ($cagwInstanceDescription): $cagwCurrentSubscribers . Maximum Allowed: $cagwMaximumSubscribers . Utilization $BWGSubscribersUtilizationPercent%.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
BWGSubscribersThreshold	Indicates the utilization of the BWG Gateway. - Critical: 100% utilized. The maximum number of subscribers that can be concurrently supported by this BWG has been reached. - Major: Between 90% to 100% utilized [90%-100%). - Warning: Between 80% to 90% utilized [80%-90%). - Normal: Less than 80% utilized [0%-80%).
cagwCurrentSubscribers	The number of subscribers currently connected to this BWG.
cagwMaximumSubscribers	The maximum number of base stations that can be concurrently supported by this BWG.
BWGSubscribersThresholdPercent	The ratio of cagwCurrentSubscribers / cagwMaximumSubscribers expressed as a percent.
cagwInstanceDescription	Description of the physical instance of the BWG.
cagwInstanceIndex	An index that uniquely represents each BWG per device. This index is assigned arbitrarily by the engine and is not saved over reboots.

Operational Information:

Go Top

SECTION 1.3

Trap: ciscoAgwMaxBaseStationExceededOnsetNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BWGMaxBaseStationExceededOnset	Trap	Event	No	Critical	$NodeDisplayName - The number of base stations ($cagwCurrentBaseStations) exceeded a threshold. The maximum allowed is $cagwMaximumBaseStations.	BWGMaxBaseStationExceededOnset	BWG
BWGMaxBaseStationExceededOnset	Trap	Event	No	Major	$NodeDisplayName - The number of base stations ($cagwCurrentBaseStations) exceeded a threshold. The maximum allowed is $cagwMaximumBaseStations.	BWGMaxBaseStationExceededOnset	BWG
BWGMaxBaseStationExceededOnset	Trap	Event	No	Minor	$NodeDisplayName - The number of base stations ($cagwCurrentBaseStations) exceeded a threshold. The maximum allowed is $cagwMaximumBaseStations.	BWGMaxBaseStationExceededOnset	BWG

BWGMaxBaseStationExceededOnset	Trap	Event	No	Warning	$NodeDisplayName - The number of base stations ($cagwCurrentBaseStations) exceeded a threshold. The maximumx allowed is $cagwMaximumBaseStations.	BWGMaxBaseStationExceededOnset	BWG
BWGMaxBaseStationExceededOnset	Trap	Event	No	Informational	$NodeDisplayName - The number of base stations ($cagwCurrentBaseStations) exceeded a threshold. The maximum allowed is $cagwMaximumBaseStations.	BWGMaxBaseStationExceededOnset	BWG

Description:

```
A notification of this type is generated when
the number of base stations exceeded the
percent of the maximum number of base stations
as specified by the object
cagwMaxBaseStationExceededNotifThreshold.
```

Default Message:

$NodeDisplayName - The number of base stations ($cagwCurrentBaseStations) exceeded a threshold. The maximum allowed is $cagwMaximumBaseStations.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cagwInstanceDescription	Description of the physical instance of the BWG.
cagwMaxBaseStationExceededNotifSeverity	Indicates the severity of the ciscoAgwMaxBaseStationExceededOnsetNotif notification. The severity of ciscoAgwMaxBaseStationExceededAbateNotif is 'cleared'. This object cannot be set to cleared(1) or indeterminate(2).
cagwMaximumBaseStations	The maximum number of base stations that can be concurrently supported by this BWG.
cagwCurrentBaseStations	The current number of signaling paths to all Base Stations. There is one signaling path created between the BWG and each base station, so the current number of signaling paths is equal to the number of base stations currently connected to the BWG. Signaling paths and base stations are used interchangeably throughout this document.
cagwRejectedBaseStations	The number of paths that were rejected due to exceeding the maximum number of base stations allowed to connect to this BWG. See object cagwMaximumBaseStations.
cagwImpactedIpType	This object provides the type of the address contained in the cagwImpactedIp object.
cagwImpactedIp	This is the address of the device impacted by the event that caused the generation of the notification containing this object.

Go Top

Trap: ciscoAgwServiceUpNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BWGServiceUp	Trap	Event	No	Informational	$NodeDisplayName - BWG $cagwInstanceDescription is in service.	BWGServiceUp	BWG

Description:

```
A notification of this type is generated when
the BWG is in service.
```

Default Message:

$NodeDisplayName - BWG gateway $cagwInstanceDescription is in service.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cagwInstanceDescription	Description of the physical instance of the BWG.
cagwServiceNotifSeverity	Indicates the severity of the ciscoAgwServiceDownNotif notification. The severity of ciscoAgwServiceUpNotif is 'cleared'. This object cannot be set to cleared(1) or indeterminate(2).

Go Top

SECTION 1.5

Trap: ciscoAgwServiceDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BWGServiceDown	Trap	Event	No	Critical	$NodeDisplayName - BWG $cagwInstanceDescription is not in service.	BWGServiceDown	BWG
BWGServiceDown	Trap	Event	No	Major	$NodeDisplayName - BWG $cagwInstanceDescription is not in service.	BWGServiceDown	BWG
BWGServiceDown	Trap	Event	No	Minor	$NodeDisplayName - BWG $cagwInstanceDescription is not in service.	BWGServiceDown	BWG
BWGServiceDown	Trap	Event	No	Warning	$NodeDisplayName - BWG $cagwInstanceDescription is not in service.	BWGServiceDown	BWG
BWGServiceDown	Trap	Event	No	Informational	$NodeDisplayName - BWG $cagwInstanceDescription is not in service.	BWGServiceDown	BWG

Description:

```
A notification of this type is generated when
the BWG is not in service.
```

Default Message:

$NodeDisplayName - BWG $cagwInstanceDescription is not in service.

Message Substitution Variables:

Common	Substitution variables common to all traps.
	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
cagwInstanceDescription	Description of the physical instance of the BWG.
cagwServiceNotifSeverity	Indicates the severity of the ciscoAgwServiceDownNotif notification. The severity of ciscoAgwServiceUpNotif is 'cleared'. This object cannot be set to cleared(1) or indeterminate(2).

Go Top

SECTION 1.6

Trap: ciscoAgwMaxSubscribersExceededOnsetNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BWGMaxSubscribersExceededOnset	Trap	Event	No	Critical	$NodeDisplayName - The number of subscribers ($cagwCurrentSubscribers) exceeded a threshold. The maximum allowed is $cagwMaximumSubscribers .	BWGMaxSubscribersExceededOnset	BWG
BWGMaxSubscribersExceededOnset	Trap	Event	No	Major	$NodeDisplayName - The number of subscribers ($cagwCurrentSubscribers) exceeded a threshold. The maximum allowed is $cagwMaximumSubscribers .	BWGMaxSubscribersExceededOnset	BWG
BWGMaxSubscribersExceededOnset	Trap	Event	No	Minor	$NodeDisplayName - The number of subscribers ($cagwCurrentSubscribers) exceeded a threshold. The maximum allowed is $cagwMaximumSubscribers .	BWGMaxSubscribersExceededOnset	BWG
BWGMaxSubscribersExceededOnset	Trap	Event	No	Warning	$NodeDisplayName - The number of subscribers ($cagwCurrentSubscribers) exceeded a threshold. The maximum allowed is $cagwMaximumSubscribers .	BWGMaxSubscribersExceededOnset	BWG
BWGMaxSubscribersExceededOnset	Trap	Event	No	Informational	$NodeDisplayName - The number of subscribers ($cagwCurrentSubscribers) exceeded a threshold. The maximum allowed is $cagwMaximumSubscribers .	BWGMaxSubscribersExceededOnset	BWG

Description:

A notification of this type is generated when
the number of subscribers exceeded the
percent of the maximum number of base stations
as specified by the object
cagwMaxSubscribersExceededNotifThreshold.

Default Message:

$NodeDisplayName - The number of subscribers ($cagwCurrentSubscribers
) exceeded a threshold. The maximum allowed is
$cagwMaximumSubscribers .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cagwInstanceDescription	Description of the physical instance of the BWG.
	Indicates the severity of the

cagwMaxSubscribersExceededNotifSeverity	ciscoAgwMaxSubscribersExceededOnsetNotif notification. The severity of ciscoAgwMaxSubscribersExceededAbateNotif is 'cleared'. This object cannot be set to cleared(1) or indeterminate(2).
cagwMaximumSubscribers	The maximum number of subscribers that can be concurrently supported by this BWG.
cagwCurrentSubscribers	The number of subscribers currently connected to this BWG.
cagwRejectedSessions	The number of sessions that were rejected due to exceeding the maximum number of allowed subscribers. See object cagwMaximumSubscribers.
cagwImpactedIpType	This object provides the type of the address contained in the cagwImpactedIp object.
cagwImpactedIp	This is the address of the device impacted by the event that caused the generation of the notification containing this object.

Go Top

SECTION 1.7

Trap: ciscoAgwMaxBaseStationExceededAbateNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BWGMaxBaseStationExceededAbate	Trap	Event	No	Normal	$NodeDisplayName - The number of base stations ($cagwCurrentBaseStations) is within normal tolerances.	BWGMaxBaseStationExceededAbate	BWG

Description:

A notification of this type is generated when
the number of base stations goes below the
percent of the maximum number of base stations
as specified by the object
cagwMaxBaseStationExceededNotifThreshold.

Default Message:

$NodeDisplayName - The number of base stations ($cagwCurrentBaseStations) is within normal tolerances.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cagwInstanceDescription	Description of the physical instance of the BWG.
cagwMaxBaseStationExceededNotifSeverity	Indicates the severity of the ciscoAgwMaxBaseStationExceededOnsetNotif notification. The severity of ciscoAgwMaxBaseStationExceededAbateNotif is 'cleared'. This object cannot be set to cleared(1) or indeterminate(2).
cagwMaximumBaseStations	The maximum number of base stations that can be concurrently supported by this BWG.

cagwCurrentBaseStations	The current number of signaling paths to all Base Stations. There is one signaling path created between the BWG and each base station, so the current number of signaling paths is equal to the number of base stations currently connected to the BWG. Signaling paths and base stations are used interchangeably throughout this document.
cagwRejectedBaseStations	The number of paths that were rejected due to exceeding the maximum number of base stations allowed to connect to this BWG. See object cagwMaximumBaseStations.

Go Top

SECTION 1.8

Trap: ciscoAgwMaxSubscribersExceededAbateNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BWGMaxSubscribersExceededAbate	Trap	Event	No	Normal	$NodeDisplayName - The number of subscribers ($cagwCurrentSubscribers) is within normal tolerances.	BWGMaxSubscribersExceededAbate	BWG

Description:

A notification of this type is generated when the number of subscribers goes below the percent of the maximum number of base stations as specified by the object cagwMaxSubscribersExceededNotifThreshold.

Default Message:

$NodeDisplayName - The number of subscribers ($cagwCurrentSubscribers) is within normal tolerances.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cagwInstanceDescription	Description of the physical instance of the BWG.
cagwMaxSubscribersExceededNotifSeverity	Indicates the severity of the ciscoAgwMaxSubscribersExceededOnsetNotif notification. The severity of ciscoAgwMaxSubscribersExceededAbateNotif is 'cleared'. This object cannot be set to cleared(1) or indeterminate(2).
cagwMaximumSubscribers	The maximum number of subscribers that can be concurrently supported by this BWG.
cagwCurrentSubscribers	The number of subscribers currently connected to this BWG.
cagwRejectedSessions	The number of sessions that were rejected due to exceeding the maximum number of allowed subscribers. See object cagwMaximumSubscribers.

Go Top

SECTION 2.1

Trap: ciscoCsgQuotaMgrLostRecordEvent

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgQuotaMgrRecordsLost	Trap	Alarm	No	Warning	$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the quota manager.	CsgQuotaMgrRecordsLost	CSG1

Description:

```
This notification is issued when csgQuotaNotifsEnabled            is set to 'true', and the CSG must discard request
records to be sent to the quota manager. The processing
is the same as described in the description for
ciscoCsgAgentLostRecordEvent.
```

Default Message:

$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the quota manager.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgQuotaMgrState	States of a quota manager: 'standby' - The QuotaMgr is prepared to become active. 'failed' - The QuotaMgr has failed to respond to requests. 'active' - The QuotaMgr has been activated to receive requests. 'echowait' - CSG has sent an echo request to this QuotaMgr and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this QuotaMgr and is waiting for a response. 'suspended' - The QuotaMgr has receive a stop request from the operator.
csgQuotaMgrLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgQuotaMgrTotalSent	Total number of records sent to the quota manager.
csgQuotaMgrFailAck	Number of acknowledgments received from the quota manager for which there are no requests.
csgQuotaMgrOutstanding	Current number of messages waiting to be ACKed.
csgQuotaMgrHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgQuotaMgrBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgQuotaMgrRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.2

Trap: ciscoCsgUserDbStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgUserDbReset	Trap	Alarm	No	Minor	$NodeDisplayName -- The CSG user database is reset.	CsgUserDbReset	CSG1

Description:

```
This notification is issued when csgDatabaseNotifsEnabled            is set to 'true', and the user database changes state.
```

Default Message:

$NodeDisplayName -- The CSG user database failed to respond to requests.
$NodeDisplayName -- The CSG user database is active.
$NodeDisplayName -- The CSG user database is reset.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgUserDbState	State of the user database. 'reset' - State before the database is determined to be active. 'active' - The database is available and processing requests. 'failed' - The database has failed and is not processing requests.
csgUserDbRequests	Number of user database requests.
csgUserDbUidsReturned	Number of user identifiers returned.
csgUserDbReqResent	Number of database requests resent.
csgUserDbReqTimeouts	Number of user database requests that have timed out.
csgUserDbReqErrors	Number of errors returned on user database requests.

Go Top

SECTION 2.3

Trap: ciscoCsgAgentLostRecordEvent

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgBMALostRecord	Trap	Alarm	No	Warning	$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the BMA.	CsgBMALostRecord	CSG1

Description:

```
This notification is issued when csgAgentNotifsEnabled            is set to 'true', and the CSG must discard accounting
records that should be sent to the billing mediation
agent.
Initially, csgAgentLostRecords is set to 0.
When a record is discarded, csgAgentLostRecords
is incremented, a period timer is started, and this
notification is issued. The NMS and the agent save
this value. The agent continues to increment
csgAgentLostRecords each time a record is lost.
When the period timer expires, the agent compares
the current value of csgAgentLostRecords with
the previous (saved) value. If the values are equal
this notification is issued again, signalling to the
NMS that the condition has been cleared. Otherwise,
```

```
the timer is restarted to monitor the next period.
When a record is lost and no period timer is active,
this notification is issued and the above procedure
is repeated.
```

Default Message:

$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the BMA.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgAgentState	States of a billing mediation agent. 'standby' - The server is prepared to become active. 'failed' - The server has failed to respond to requests. 'active' - The server has been activated to receive requests. 'echowait' - CSG has sent an echo request to this billing mediation agent and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this billing mediation agent and is waiting for a response. 'suspended' - The server has receive a stop request from the operator.
csgAgentLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgAgentTotalSent	Total number of records sent to the billing mediation agent.
csgAgentFailAck	Number of acknowledgments received from the billing mediation agent for which there are no outstanding requests.
csgAgentOutstanding	Current number of messages waiting to be ACKed.
csgAgentHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgAgentBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgAgentRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.4

Trap: ciscoCsgQuotaMgrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgQuotaMgrStandby	Trap	Alarm	No	Minor	$NodeDisplayName -- The quota manager server is prepared to become active.	CsgQuotaMgrStandby	CSG1

Description:

```
This notification is issued when csgQuotaNotifsEnabled            is set to 'true', and the quota manager changes state.
There is one exception: No notification is issued for
state changes involving 'echowait' because this would
cause an excessive number of notifications.
```

Default Message:

$NodeDisplayName -- The quota manager server is prepared to become active.
$NodeDisplayName -- The quota manager server failed to respond to requests.
$NodeDisplayName -- The CSG sent a node-alive request to this quota manager and is waiting for a response.
$NodeDisplayName -- The quota manager is suspended by the operator.
$NodeDisplayName -- The quota manager is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgQuotaMgrState	States of a quota manager: 'standby' - The QuotaMgr is prepared to become active. 'failed' - The QuotaMgr has failed to respond to requests. 'active' - The QuotaMgr has been activated to receive requests. 'echowait' - CSG has sent an echo request to this QuotaMgr and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this QuotaMgr and is waiting for a response. 'suspended' - The QuotaMgr has receive a stop request from the operator.
csgQuotaMgrLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgQuotaMgrTotalSent	Total number of records sent to the quota manager.
csgQuotaMgrFailAck	Number of acknowledgments received from the quota manager for which there are no requests.
csgQuotaMgrOutstanding	Current number of messages waiting to be ACKed.
csgQuotaMgrHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgQuotaMgrBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgQuotaMgrRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.5

Trap: ciscoCsgAgentStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgBMAStandby	Trap	Alarm	No	Minor	$NodeDisplayName -- The BMA is prepared to become active.	CsgBMAStandby	CSG1

Description:

This notification is issued when csgAgentNotifsEnabled is set to 'true', and the billing mediation agent changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.

Default Message:

$NodeDisplayName -- The BMA is prepared to become active.

$NodeDisplayName -- BMA server failed to respond to the CSG.
$NodeDisplayName -- The CSG sent a node-alive request to this BMA and is waiting for a response.
$NodeDisplayName -- The BMA is suspended by the operator.
$NodeDisplayName -- The BMA is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgAgentState	States of a billing mediation agent. 'standby' - The server is prepared to become active. 'failed' - The server has failed to respond to requests. 'active' - The server has been activated to receive requests. 'echowait' - CSG has sent an echo request to this billing mediation agent and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this billing mediation agent and is waiting for a response. 'suspended' - The server has receive a stop request from the operator.
csgAgentLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgAgentTotalSent	Total number of records sent to the billing mediation agent.
csgAgentFailAck	Number of acknowledgments received from the billing mediation agent for which there are no outstanding requests.
csgAgentOutstanding	Current number of messages waiting to be ACKed.
csgAgentHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgAgentBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgAgentRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.6

Trap: ciscoCsgAgentStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgBMAFailed	Trap	Alarm	No	Major	$NodeDisplayName -- BMA server failed to respond to the CSG.	CsgBMAFailed	CSG1

Description:

This notification is issued when csgAgentNotifsEnabled is set to 'true', and the billing mediation agent changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.

Default Message:

$NodeDisplayName -- The BMA is prepared to become active.
$NodeDisplayName -- BMA server failed to respond to the CSG.

$NodeDisplayName -- The CSG sent a node-alive request to this BMA and is waiting for a response.
$NodeDisplayName -- The BMA is suspended by the operator.
$NodeDisplayName -- The BMA is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgAgentState	States of a billing mediation agent. 'standby' - The server is prepared to become active. 'failed' - The server has failed to respond to requests. 'active' - The server has been activated to receive requests. 'echowait' - CSG has sent an echo request to this billing mediation agent and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this billing mediation agent and is waiting for a response. 'suspended' - The server has receive a stop request from the operator.
csgAgentLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgAgentTotalSent	Total number of records sent to the billing mediation agent.
csgAgentFailAck	Number of acknowledgments received from the billing mediation agent for which there are no outstanding requests.
csgAgentOutstanding	Current number of messages waiting to be ACKed.
csgAgentHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgAgentBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgAgentRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.7

Trap: ciscoCsgAgentStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgBMANAWait	Trap	Alarm	No	Minor	$NodeDisplayName -- The CSG sent a node-alive request to this BMA and is waiting for a response.	CsgBMANAWait	CSG1

Description:

This notification is issued when csgAgentNotifsEnabled is set to 'true', and the billing mediation agent changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.

Default Message:

$NodeDisplayName -- The BMA is prepared to become active.
$NodeDisplayName -- BMA server failed to respond to the CSG.
$NodeDisplayName -- The CSG sent a node-alive request to this BMA and is waiting for a response.

$NodeDisplayName -- The BMA is suspended by the operator.
$NodeDisplayName -- The BMA is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgAgentState	States of a billing mediation agent. 'standby' - The server is prepared to become active. 'failed' - The server has failed to respond to requests. 'active' - The server has been activated to receive requests. 'echowait' - CSG has sent an echo request to this billing mediation agent and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this billing mediation agent and is waiting for a response. 'suspended' - The server has receive a stop request from the operator.
csgAgentLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgAgentTotalSent	Total number of records sent to the billing mediation agent.
csgAgentFailAck	Number of acknowledgments received from the billing mediation agent for which there are no outstanding requests.
csgAgentOutstanding	Current number of messages waiting to be ACKed.
csgAgentHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgAgentBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgAgentRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.8

Trap: ciscoCsgAgentStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgBMASuspended	Trap	Alarm	No	Major	$NodeDisplayName -- The BMA is suspended by the operator.	CsgBMASuspended	CSG1

Description:

This notification is issued when csgAgentNotifsEnabled is set to 'true', and the billing mediation agent changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.

Default Message:

$NodeDisplayName -- The BMA is prepared to become active.
$NodeDisplayName -- BMA server failed to respond to the CSG.
$NodeDisplayName -- The CSG sent a node-alive request to this BMA and is waiting for a response.
$NodeDisplayName -- The BMA is suspended by the operator.

$NodeDisplayName -- The BMA is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgAgentState	States of a billing mediation agent. 'standby' - The server is prepared to become active. 'failed' - The server has failed to respond to requests. 'active' - The server has been activated to receive requests. 'echowait' - CSG has sent an echo request to this billing mediation agent and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this billing mediation agent and is waiting for a response. 'suspended' - The server has receive a stop request from the operator.
csgAgentLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgAgentTotalSent	Total number of records sent to the billing mediation agent.
csgAgentFailAck	Number of acknowledgments received from the billing mediation agent for which there are no outstanding requests.
csgAgentOutstanding	Current number of messages waiting to be ACKed.
csgAgentHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgAgentBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgAgentRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.9

Trap: ciscoCsgAgentStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgBMAActive	Trap	Alarm	No	Normal	$NodeDisplayName -- The BMA is active.	CsgBMAActive	CSG1

Description:

This notification is issued when csgAgentNotifsEnabled is set to 'true', and the billing mediation agent changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.

Default Message:

$NodeDisplayName -- The BMA is prepared to become active.
$NodeDisplayName -- BMA server failed to respond to the CSG.
$NodeDisplayName -- The CSG sent a node-alive request to this BMA and is waiting for a response.
$NodeDisplayName -- The BMA is suspended by the operator.
$NodeDisplayName -- The BMA is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgAgentState	States of a billing mediation agent. 'standby' - The server is prepared to become active. 'failed' - The server has failed to respond to requests. 'active' - The server has been activated to receive requests. 'echowait' - CSG has sent an echo request to this billing mediation agent and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this billing mediation agent and is waiting for a response. 'suspended' - The server has receive a stop request from the operator.
csgAgentLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgAgentTotalSent	Total number of records sent to the billing mediation agent.
csgAgentFailAck	Number of acknowledgments received from the billing mediation agent for which there are no outstanding requests.
csgAgentOutstanding	Current number of messages waiting to be ACKed.
csgAgentHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgAgentBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgAgentRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.10

Trap: ciscoCsgQuotaMgrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgQuotaMgrFailed	Trap	Alarm	No	Major	$NodeDisplayName -- The quota manager server failed to respond to requests.	CsgQuotaMgrFailed	CSG1

Description:

This notification is issued when csgQuotaNotifsEnabled is set to 'true', and the quota manager changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.

Default Message:

$NodeDisplayName -- The quota manager server is prepared to become active.
$NodeDisplayName -- The quota manager server failed to respond to requests.
$NodeDisplayName -- The CSG sent a node-alive request to this quota manager and is waiting for a response.
$NodeDisplayName -- The quota manager is suspended by the operator.
$NodeDisplayName -- The quota manager is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgQuotaMgrState	States of a quota manager: 'standby' - The QuotaMgr is prepared to become active. 'failed' - The QuotaMgr has failed to respond to requests. 'active' - The QuotaMgr has been activated to receive requests. 'echowait' - CSG has sent an echo request to this QuotaMgr and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this QuotaMgr and is waiting for a response. 'suspended' - The QuotaMgr has receive a stop request from the operator.
csgQuotaMgrLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgQuotaMgrTotalSent	Total number of records sent to the quota manager.
csgQuotaMgrFailAck	Number of acknowledgments received from the quota manager for which there are no requests.
csgQuotaMgrOutstanding	Current number of messages waiting to be ACKed.
csgQuotaMgrHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgQuotaMgrBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgQuotaMgrRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.11

Trap: ciscoCsgQuotaMgrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgQuotaMgrNAWait	Trap	Alarm	No	Minor	$NodeDisplayName -- The CSG sent a node-alive request to this quota manager and is waiting for a response.	CsgQuotaMgrNAWait	CSG1

Description:

This notification is issued when csgQuotaNotifsEnabled is set to 'true', and the quota manager changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.

Default Message:

$NodeDisplayName -- The quota manager server is prepared to become active.
$NodeDisplayName -- The quota manager server failed to respond to requests.
$NodeDisplayName -- The CSG sent a node-alive request to this quota manager and is waiting for a response.
$NodeDisplayName -- The quota manager is suspended by the operator.
$NodeDisplayName -- The quota manager is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgQuotaMgrState	States of a quota manager: 'standby' - The QuotaMgr is prepared to become active. 'failed' - The QuotaMgr has failed to respond to requests. 'active' - The QuotaMgr has been activated to receive requests. 'echowait' - CSG has sent an echo request to this QuotaMgr and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this QuotaMgr and is waiting for a response. 'suspended' - The QuotaMgr has receive a stop request from the operator.
csgQuotaMgrLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgQuotaMgrTotalSent	Total number of records sent to the quota manager.
csgQuotaMgrFailAck	Number of acknowledgments received from the quota manager for which there are no requests.
csgQuotaMgrOutstanding	Current number of messages waiting to be ACKed.
csgQuotaMgrHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgQuotaMgrBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgQuotaMgrRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.12

Trap: ciscoCsgQuotaMgrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgQuotaMgrSuspended	Trap	Alarm	No	Major	$NodeDisplayName -- The quota manager is suspended by the operator.	CsgQuotaMgrSuspended	CSG1

Description:

This notification is issued when csgQuotaNotifsEnabled is set to 'true', and the quota manager changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.

Default Message:

$NodeDisplayName -- The quota manager server is prepared to become active.
$NodeDisplayName -- The quota manager server failed to respond to requests.
$NodeDisplayName -- The CSG sent a node-alive request to this quota manager and is waiting for a response.
$NodeDisplayName -- The quota manager is suspended by the operator.
$NodeDisplayName -- The quota manager is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
csgQuotaMgrState	States of a quota manager: 'standby' - The QuotaMgr is prepared to become active. 'failed' - The QuotaMgr has failed to respond to requests. 'active' - The QuotaMgr has been activated to receive requests. 'echowait' - CSG has sent an echo request to this QuotaMgr and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this QuotaMgr and is waiting for a response. 'suspended' - The QuotaMgr has receive a stop request from the operator.
csgQuotaMgrLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgQuotaMgrTotalSent	Total number of records sent to the quota manager.
csgQuotaMgrFailAck	Number of acknowledgments received from the quota manager for which there are no requests.
csgQuotaMgrOutstanding	Current number of messages waiting to be ACKed.
csgQuotaMgrHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgQuotaMgrBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgQuotaMgrRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

SECTION 2.13

Trap: ciscoCsgUserDbStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgUserDbFailed	Trap	Alarm	No	Major	$NodeDisplayName -- The CSG user database failed to respond to requests.	CsgUserDbFailed	CSG1

Description:

This notification is issued when csgDatabaseNotifsEnabled is set to 'true', and the user database changes state.

Default Message:

$NodeDisplayName -- The CSG user database failed to respond to requests.
$NodeDisplayName -- The CSG user database is active.
$NodeDisplayName -- The CSG user database is reset.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgUserDbState	State of the user database. 'reset' - State before the database is determined to be active. 'active' - The database is available and processing requests. 'failed' - The database has failed and is not processing requests.

csgUserDbRequests	Number of user database requests.
csgUserDbUidsReturned	Number of user identifiers returned.
csgUserDbReqResent	Number of database requests resent.
csgUserDbReqTimeouts	Number of user database requests that have timed out.
csgUserDbReqErrors	Number of errors returned on user database requests.

Go Top

SECTION 2.14

Trap: ciscoCsgUserDbStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgUserDbActive	Trap	Alarm	No	Normal	$NodeDisplayName -- The CSG user database is active.	CsgUserDbActive	CSG1

Description:

This notification is issued when csgDatabaseNotifsEnabled is set to 'true', and the user database changes state.

Default Message:

$NodeDisplayName -- The CSG user database failed to respond to requests.
$NodeDisplayName -- The CSG user database is active.
$NodeDisplayName -- The CSG user database is reset.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgUserDbState	State of the user database. 'reset' - State before the database is determined to be active. 'active' - The database is available and processing requests. 'failed' - The database has failed and is not processing requests.
csgUserDbRequests	Number of user database requests.
csgUserDbUidsReturned	Number of user identifiers returned.
csgUserDbReqResent	Number of database requests resent.
csgUserDbReqTimeouts	Number of user database requests that have timed out.
csgUserDbReqErrors	Number of errors returned on user database requests.

Go Top

SECTION 2.15

Trap: ciscoCsgQuotaMgrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgQuotaMgrActive	Trap	Alarm	No	Normal	$NodeDisplayName -- The quota manager is active.	CsgQuotaMgrActive	CSG1

Description:

```
This notification is issued when csgQuotaNotifsEnabled            is set to 'true', and the quota manager changes state.
There is one exception: No notification is issued for
state changes involving 'echowait' because this would
cause an excessive number of notifications.
```

Default Message:

$NodeDisplayName -- The quota manager server is prepared to become active.
$NodeDisplayName -- The quota manager server failed to respond to requests.
$NodeDisplayName -- The CSG sent a node-alive request to this quota manager and is waiting for a response.
$NodeDisplayName -- The quota manager is suspended by the operator.
$NodeDisplayName -- The quota manager is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
csgQuotaMgrState	States of a quota manager: 'standby' - The QuotaMgr is prepared to become active. 'failed' - The QuotaMgr has failed to respond to requests. 'active' - The QuotaMgr has been activated to receive requests. 'echowait' - CSG has sent an echo request to this QuotaMgr and is waiting for a response. 'nawait' - CSG has sent a node-alive request to this QuotaMgr and is waiting for a response. 'suspended' - The QuotaMgr has receive a stop request from the operator.
csgQuotaMgrLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
csgQuotaMgrTotalSent	Total number of records sent to the quota manager.
csgQuotaMgrFailAck	Number of acknowledgments received from the quota manager for which there are no requests.
csgQuotaMgrOutstanding	Current number of messages waiting to be ACKed.
csgQuotaMgrHighWater	Highest number of messages waiting for ACKs. The only write operation allowed is to reset the value to 0.
csgQuotaMgrBadRecord	The number of bad records received. These are records in which the CSG detected an error in attempting to decode the contents.
csgQuotaMgrRetransmit	The number of messages retransmitted to the billing mediation agent.

Go Top

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 2.16

Status: SystemTraffic

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SystemTraffic	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The system traffic threshold is Acceptable. Value $SystemTrafficValue	SystemTraffic	CSG1
SystemTraffic	Poll	Alarm	Yes	Major	$NodeDisplayName -- The system traffic threshold is Exceeded. Value $SystemTrafficValue	SystemTraffic	CSG1

Description:

Traffic meter value, i.e. the percentage of bandwidth utilization for the previous polling interval.

Default Message:

$NodeDisplayName -- The system traffic threshold is $SystemTrafficState. Value $SystemTrafficValue

Message Substitution Variables:

Node	Substitution variables for Node related data.
SystemTrafficState	Acceptable or Exceeded
SystemTrafficValue	The value of sysTraffic

Go Top

SECTION 3.1

Trap: ciscoContentServicesUserThresholdExceeded

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CsgLicenseLimit	Trap	Alarm	Yes	Major	$NodeDisplayName -- The CSG license limit is reached. The number of users $ccsgsUserCurrent is above threshold $ccsgsUserThreshold. User highwater mark $ccsgsUserHighWater.	CsgLicenseLimit	CSG2
CsgLicenseLimit	Poll	Alarm	Yes	Major	$NodeDisplayName -- The CSG license limit is reached. The number of users $ccsgsUserCurrent is above threshold $ccsgsUserThreshold. User highwater mark $ccsgsUserHighWater.	CsgLicenseLimit	CSG2
CsgLicenseLimit	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The number of users $ccsgsUserCurrent is below threshold $ccsgsUserThreshold. User highwater mark $ccsgsUserHighWater.	CsgLicenseLimit	CSG2

Description:

This notification is issued when ccsUserThresholdExceededNotifEnabled is set to 'true', and when actual users limit exceeds threshold which is set by ccsgsUserThreshold.

Default Message:

$NodeDisplayName -- The CSG license limit is reached. The number of users $ccsgsUserCurrent is above threshold $ccsgsUserThreshold. User highwater mark $ccsgsUserHighWater.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccsgsUserCurrent	The total number of users with one or more active sessions on the system.
ccsgsUserHighWater	The highest number of active users as reported by ccsgsUserCurrent object since the object was reset as indicated by ccsgsUserHighWaterResetTime. The only write operation allowed is to reset the value to 0.
ccsgsUserThreshold	The maximum number of users that is contractually

	allowed. When the actual number of user exceeds the contractually established limit, a notification (ciscoContentServicesUserThresholdExceeded) is issued.
entPhysicalIndex	The index for this entry.

Go Top

SECTION 3.2

Trap: ciscoContentServicesQuotaMgrLostRecordEvent

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
QuotaMgrLostRecords	Trap	Alarm	No	Major	$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the Quota Manager $ccsQuotaMgrState_ccsQuotaMgrIpAddr:$ccsQuotaMgrState_ccsQuotaMgrPort:$ccsQuotaMgrState_ccsQuotaMgrVrfName.	QuotaMgrLostRecords	CSG2
QuotaMgrLostRecords	Poll	Alarm	No	Major	$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the Quota Manager $QuotaMgrIpAddr:$QuotaMgrPort:$QuotaMgrVrfName.	QuotaMgrLostRecords	CSG2

Description:

```
This notification is issued when ccsQuotaMgrStateChangeNotifEnabled        is set to 'true', and request records to be sent to the
quota manager must be discarded. The processing
is the same as described in the description for
ccsQuotaMgrLostRecordEvent.
```

Default Message:

$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the quota manager in active state.
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the quota manager in echowait state.
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the quota manager in failed state.
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the quota manager in nawait state.
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the quota manager in standby state.
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the quota manager in suspended state.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccsQuotaMgrState	States of a quota manager: 'standby' - The QuotaMgr is prepared to become active. 'failed' - The QuotaMgr has failed to respond to requests. 'active' - The QuotaMgr has been activated to receive requests. 'echowait' - An echo request to this QuotaMgr and is waiting for a response. 'nawait' - A node-alive request to this QuotaMgr and is waiting for a response. 'suspended' - The QuotaMgr has receive a stop request from the operator.
ccsQuotaMgrLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
ccsQuotaMgrTotalSent	Total number of records sent to the quota manager.
ccsQuotaMgrFailAck	Number of acknowledgments received from the quota manager for which there are no requests.

ccsQuotaMgrOutstanding	Current number of messages waiting to be ACKed.
ccsQuotaMgrHighWater	The highest number of messages waiting for ACKs as reported by ccsQuotaMgrOutstanding object since object was reset as indicated by ccsQuotaMgrHighWaterResetTime. The only write operation allowed is to reset the value to 0.
ccsQuotaMgrBadRecord	The number of bad records received. These are records in which the an error detected while attempting to decode the contents.
ccsQuotaMgrRetransmit	The number of messages retransmitted to the billing mediation agent.

Operational Information:

This event is primarily generated when the queue between the control processor of the CSG card and the QuotaMgr is saturated. Further records need to be dropped in this scenario. A remedy would be to increase the size of this queue This event indicates a potential link failure or overload situation at the CSG device. Records may be lost due to a vareity of reasons:
1. Link failure or connection problems between CSG and QuotaMgr due to network congestion or other factors
2. Misconfiguration at the QuotaMgr
3. Overloading of CSG

Troubleshooting:

Steps to Troubleshoot:

Step 1: Session into the CSG and execute the show command : "show ip csg quota-server detail"
Step 2: If the records have been lost due to link problems,the 'retransmits' variable in the output must increase
Step 3: Link problems as the cause of lost records can be ascertained if we get the "ciscoContentServicesQuotaMgrStateChange" trap from the CSG
Step 3: If there is a misconfiguration at the QuotaMgr, the 'bad records' variable or the 'reject' variable will increase
Step 4: If there occurs an overload at the CSG the 'dropped' variable will increase
Step 5: The overload can also be detected by examining the in the output of the show command : "show ip csg verload can also be detected by examining various denials variables (IPC denials,rate denials and buffer denials) in the output of the show command : "show ip csg load"; the number of denials will be high in case of an overload.
Step 6: Turn on “debug ip csg gtp quota-server", but be aware of the performance impact
Step 7: You can view these variables by examining the statistics tab of the device in the MWTM webclient .

Go Top

SECTION 3.3

Trap: ciscoContentServicesBMALostRecordEvent

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BMALostRecords	Trap	Alarm	No	Major	$NodeDisplayName -- The CSG is discarding accounting records for BMA $ccsBMAState_ccsBMAIpAddr:$ccsBMAState_ccsBMAPort:$ccsBMAState_ccsBMAVrfName.	BMALostRecords	CSG2
BMALostRecords	Poll	Alarm	No	Major	$NodeDisplayName -- The CSG is discarding accounting records for BMA $BMAIpAddr:$BMAPort:$BMAVrfName.	BMALostRecords	CSG2

Description:

This notification is issued when ccsBMAStateChangeNotifEnabled is set to 'true', and accounting records, should be sent to the billing mediation agent, must be discarded.
Initially, ccsBMALostRecords is set to 0.
When a record is discarded, ccsBMALostRecords is incremented, a period timer is started, and this notification is issued. The NMS and the agent save this value. The agent continues to increment ccsBMALostRecords each time a record is lost.
When the period timer expires, the agent compares the current value of ccsBMALostRecords with the previous (saved) value. If the values are equal this notification is issued again, signalling to the NMS that the condition has been cleared. Otherwise, the timer is restarted to monitor the next period.
When a record is lost and no period timer is active, this notification is issued and the above procedure is repeated.

Default Message:

$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the BMA in active state
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the BMA in echowait state
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the BMA in failed state
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the BMA in nawaitstate
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the BMA in standby state
$NodeDisplayName -- The CSG is discarding accounting records that were supposed to be sent to the BMA in suspended state

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccsBMAState	States of a billing mediation agent. 'standby' - The server is prepared to become active. 'failed' - The server has failed to respond to requests. 'active' - The server has been activated to receive requests. 'echowait' - An echo request to this billing mediation agent and is waiting for a response. 'nawait' - A node-alive request to this billing mediation agent and is waiting for a response. 'suspended' - The server has receive a stop request from the operator.
ccsBMALostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
ccsBMATotalSent	Total number of records sent to the billing mediation agent.
ccsBMAFailAck	Number of acknowledgments received from the billing mediation agent for which there are no outstanding requests.
ccsBMAOutstanding	Current number of messages waiting to be ACKed.
ccsBMAHighWater	The highest number of messages waiting for ACKs as reported by ccsBMAOutstanding object since object was reset as indicated by ccsBMAHighWaterResetTime. The only write operation allowed is to reset the value to 0.
ccsBMABadRecord	The number of bad records received. These are records in which an error was detected while attempting to decode the contents.
ccsBMARetransmit	The number of messages retransmitted to the billing mediation agent.

OperationalInformation:

This event is primarily generated when the queue between the control processor of the CSG card and the BMA is saturated. Further records need to be dropped in this scenario. A remedy would be to increase the size of this queue.This event indicates a potential link failure or overload situation at the CSG device. Records may be lost due to a vareity of reasons:
1. Link failure or connection problems between CSG and BMA due to network congestion or other factors
2. Misconfiguration at the BMA
3. Overloading of CSG

Troubleshooting:

Steps to Troubleshoot:

Step 1: Session into the CSG and execute the show command : "show ip csg bma detail"
Step 2: If the records have been lost due to link problems,the 'retransmits' variable in the output must increase
Step 3: Link problems as the cause of lost records can be ascertained if we get the "ciscoContentServicesBMAStateChange" trap from the CSG
Step 3: If there is a misconfiguration at the BMA, the 'bad records' variable or the 'reject' variable will increase
Step 4: If there occurs an overload at the CSG the 'dropped' variable will increase
Step 5: The overload can also be detected by examining various denials variables (IPC denials,rate denials and buffer denials) in the output of the show command : "show ip csg load"; the number of denials will be high in case of an overload.
Step 6: Turn on “debug ip csg gtp bma", but be aware of the performance impact
Step 7: You can view these variables by examining the statistics tab of the device in the MWTM webclient

Go Top

SECTION 3.4

Trap: ciscoContentServicesUserDbStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
UserDatabaseState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The CSG user database active_ccsUserDbIpAddr:active_ccsUserDbPort:active_ccsUserDbVrfName is active.	UserDatabaseState	CSG2
UserDatabaseState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The CSG user database failed_ccsUserDbIpAddr:failed_ccsUserDbPort:failed_ccsUserDbVrfName failed to respond to requests.	UserDatabaseState	CSG2
UserDatabaseState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- The CSG user database reset_ccsUserDbIpAddr:reset_ccsUserDbPort:reset_ccsUserDbVrfName is reset.	UserDatabaseState	CSG2
UserDatabaseState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The CSG user database $UserDbIpAddr:$UserDbPort:$UserDbVrfName is active.	UserDatabaseState	CSG2
UserDatabaseState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The CSG user database $UserDbIpAddr:$UserDbPort:$UserDbVrfName failed to respond to requests.	UserDatabaseState	CSG2
UserDatabaseState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- The CSG user database $UserDbIpAddr:$UserDbPort:$UserDbVrfName is reset.	UserDatabaseState	CSG2

Description:

```
This notification is issued when ccsUserDbStateChangeNotifEnabled       is set to 'true', and the user database changes state.
```

Default Message:

$NodeDisplayName -- The CSG user database failed to respond to requests.
$NodeDisplayName -- The CSG user database is reset.
$NodeDisplayName -- The CSG user database is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccsUserDbState	State of the user database. 'reset' - State before the database is determined to be active. 'active' - The database is available and processing requests. 'failed' - The database has failed and is not processing requests.
ccsUserDbRequests	Number of user database requests.
ccsUserDbUidsReturned	Number of user identifiers returned.
ccsUserDbReqResent	Number of database requests resent.

ccsUserDbReqTimeouts	Number of user database requests that have timed out.
ccsUserDbReqErrors	Number of errors returned on user database requests.

Operational Information:

- If the state of the User database is 'Active' then no action is necessary

- If the state of the User database is 'reset' then no action is necessary.This is an indication that a User database instance is starting up either fresh or after a failure.

- If the state of the User database is 'Failed', it indicates that the server has failed to respond to requests and must be debugged for errors.

Troubleshooting:

If the state of the database server is "Failed":

Steps to Troubleshoot:

Step 1: Session into the CSG and ping the User database server.
Step 2: If ping is not successful, check routing table and CSG ARP for gateway to User database.
Step 3: If ping is successful, run the show command : show ip csg database detail.
Step 4: Observe the counter "Accrued Requests" . It should increase.
Step 4: Turn on “debug ip csg udb”, but be aware of the performance impact
Step 5: Check User database status from the server side.
Step 6: Obtain a sniffer trace on all related vlans, analyze the trace and determine the faulty party.

Go Top

SECTION 3.5

Trap: ciscoContentServicesQuotaMgrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
QuotaManagerState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The Quota Manager active_ccsQuotaMgrIpAddr:active_ccsQuotaMgrPort:active_ccsQuotaMgrVrfName is active.	QuotaManagerState	CSG2
QuotaManagerState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The Quota Manager failed_ccsQuotaMgrIpAddr:failed_ccsQuotaMgrPort:failed_ccsQuotaMgrVrfName failed to respond to requests.	QuotaManagerState	CSG2
QuotaManagerState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- The CSG sent a node-alive request to Quota Manager nawait_ccsQuotaMgrIpAddr:nawait_ccsQuotaMgrPort:nawait_ccsQuotaMgrVrfName and is waiting for a response.	QuotaManagerState	CSG2
QuotaManagerState	Trap	Alarm	Yes	Informational	$NodeDisplayName -- The Quota Manager standby_ccsQuotaMgrIpAddr:standby_ccsQuotaMgrPort:standby_ccsQuotaMgrVrfName is prepared to become active.	QuotaManagerState	CSG2
QuotaManagerState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The Quota Manager suspended_ccsQuotaMgrIpAddr:suspended_ccsQuotaMgrPort:suspended_ccsQuotaMgrVrfName is suspended by the operator.	QuotaManagerState	CSG2
QuotaManagerState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The CSG sent a echo request to Quota Manager echowait_ccsQuotaMgrIpAddr:echowait_ccsQuotaMgrPort:echowait_ccsQuotaMgrVrfName and is waiting for an echo response.	QuotaManagerState	CSG2
QuotaManagerState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The Quota Manager $QuotaMgrIpAddr:$QuotaMgrPort:$QuotaMgrVrfName is active.	QuotaManagerState	CSG2
QuotaManagerState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The Quota Manager $QuotaMgrIpAddr:$QuotaMgrPort:$QuotaMgrVrfName failed to respond to requests.	QuotaManagerState	CSG2
QuotaManagerState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- The CSG sent a node-alive request to Quota Manager $QuotaMgrIpAddr:$QuotaMgrPort:$QuotaMgrVrfName and is waiting for a response.	QuotaManagerState	CSG2
QuotaManagerState	Poll	Alarm	Yes	Informational	$NodeDisplayName -- The Quota Manager $QuotaMgrIpAddr:$QuotaMgrPort:$QuotaMgrVrfName is prepared to become active.	QuotaManagerState	CSG2
QuotaManagerState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The Quota Manager $QuotaMgrIpAddr:$QuotaMgrPort:$QuotaMgrVrfName is suspended by the operator.	QuotaManagerState	CSG2

QuotaManagerState	Poll	Alarm	Yes	Informational	$NodeDisplayName -- The CSG sent a echo request to Quota Manager $QuotaMgrIpAddr:$QuotaMgrPort:$QuotaMgrVrfName and is waiting for an echo response.	QuotaManagerState	CSG2

Description:

```
This notification is issued when ccsQuotaMgrStateChangeNotifEnabled        is set to 'true', and the quota manager changes state.
There is one exception: No notification is issued for
state changes involving 'echowait' because this would
cause an excessive number of notifications.
```

Default Message:

$NodeDisplayName -- The quota manager is active.
$NodeDisplayName -- The quota manager server failed to respond to requests.
$NodeDisplayName -- The CSG sent a node-alive request to this quota manager and is waiting for a response.
$NodeDisplayName -- The quota manager server is prepared to become active.
$NodeDisplayName -- The quota manager is suspended by the operator.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccsQuotaMgrState	States of a quota manager: 'standby' - The QuotaMgr is prepared to become active. 'failed' - The QuotaMgr has failed to respond to requests. 'active' - The QuotaMgr has been activated to receive requests. 'echowait' - An echo request to this QuotaMgr and is waiting for a response. 'nawait' - A node-alive request to this QuotaMgr and is waiting for a response. 'suspended' - The QuotaMgr has receive a stop request from the operator.
ccsQuotaMgrLostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
ccsQuotaMgrTotalSent	Total number of records sent to the quota manager.
ccsQuotaMgrFailAck	Number of acknowledgments received from the quota manager for which there are no requests.
ccsQuotaMgrOutstanding	Current number of messages waiting to be ACKed.
ccsQuotaMgrHighWater	The highest number of messages waiting for ACKs as reported by ccsQuotaMgrOutstanding object since object was reset as indicated by ccsQuotaMgrHighWaterResetTime. The only write operation allowed is to reset the value to 0.
ccsQuotaMgrBadRecord	The number of bad records received. These are records in which the an error detected while attempting to decode the contents.
ccsQuotaMgrRetransmit	The number of messages retransmitted to the billing mediation agent.

Operational Information:

- If the state of the QuotaMgr is 'Active' then no action is necessary

- If the state of the QuotaMgr is 'Stand By' then no action is necessary.This is an indication that a QuotaMgr instance had either started for the first time or had failed and the STANDBY server is ready to become Active. This must be followed by a state change to 'Active' for proper functioning.

- If the state of the QuotaMgr is 'Failed', it indicates that the QuotaMgr server has failed to respond to requests (either Echo Requests, Node Alive Requests, or Data Transfer Requests).

- If the state of a QuotaMgr is 'Echowait', it indicates that the CSG has sent an echo request to this QuotaMgr and is waiting for a response.CSG expects as reply an Echo Response message from the QuotaMgr. If the Echo Response is not received within 4 seconds, the Echo Request is resent to the QuotaMgr. "Resent" here means that the same packet is transmitted again containing the same information, sequence Number, etc. The CSG resends the Echo Request 3 times in case of no response from QuotaMgr. After the Echo Request has been sent 4 times without any reply (1st plus 3 repetitions), the CSG considers the QuotaMgr to be FAILED.

- If the state of the QuotaMgr is 'NAWAIT', it indicates that the CSG has sent a node-alive request to this QuotaMgr and is waiting for a response.CSG expects as reply a Node Alive Response message from the server (QuotaMgr). If the Node Alive Response is not received within 4 seconds, the Node Alive Request is resent to the server. "Resent" here means that the same packet is transmitted again containing same information, sequence Number, etc. The CSG resends the Node Alive Request 3 times in case of no response from server. After the Node Alive Request has been sent 4 times without any reply (1st plus 3 repetitions), the CSG considers the server to be FAILED. The CSG will send a new Node Alive Request message (new = new GTP' Sequence Number) 60 seconds after the last non-responded Node Alive Request was sent, again resending 3 times if no response is received. CSG will keep resending every 60 seconds until a Node Alive response is received from the concerned server. Once a response is received from a server, the CSG will not send any other Node Alive Request to that server unless the CSG is restarted/reloaded.

- If the state of the QuotaMgr is 'SUSPENDED', it indicates that the server has received a stop request from the operator.

Troubleshooting:

If the status of the QuotaMgr shows as "Failed","NAWAIT" or "Echowait" there is a possibility of communication failure between the CSG and the QuotaMgr.There can be two possible reasons:

1. QuotaMgr server has crashed but the link between CSG and QuotaMgr is intact

If there are standby QuotaMgr servers deployed, the failure will be repaired automatically. The failure must be followed by a state change to 'standby' and ultimately to 'Active' corresponding to the standby QuotaMgr server assuming charge.However if there are no standby servers, follow the troubleshooting steps to ascertain this.

2. Link failure between CSG and QuotaMgr or Misconfiguration at CSG

If the link between the QuotaMgr and CSG fails or if there has been a wrong configuration at the CSG on how to find the QuotaMgr, there can be a transitions to these states.

Steps to Troubleshoot:

Step 1: Session into the CSG and ping the QuotaMgr.
Step 2: If ping is not successful, check routing table and CSG ARP for gateway to QuotaMgr.
Step 3: If ping is successful, run the show command : show ip csg quota-server detail.
Step 4: Observe counters "retransmits" and "failed acks" should increase.
Step 4: Turn on "debug ip csg gtp quota-server",but be aware of the performance impact
Step 5: Check QuotaMgr status from the server side.
Step 6: Obtain a sniffer trace on all related vlans, analyze the trace and determine the faulty party.

Go Top

SECTION 3.6

Trap: cPsdClientDiskFullNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PSDDiskFull	Trap	Alarm	No	Major	$NodeDisplayName -- The PSD $cPsdClientNotifDSServerAddress disk is full. No more CDRs are being stored on the PSD.	PSDDiskFull	CSG2

Description:

```
A notification of this type is generated when the            PSD server's disk become full.
If the disk of writable PSD server becomes full, the
client shall not be able to write any CDR into the
server. It shall then  behave as a retrieve only PSD
server.
```

Default Message:

$NodeDisplayName -- The PSD disk is full. No more CDRs are being stored on the PSD.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cPsdClientNotifDSServerAddrType	This object indicates the type of Internet address of the Data-Store server.
cPsdClientNotifDSServerAddress	This object specifies the Internet address of the Data-Store server . The type of address of an instance of this object is determined by the value of cPsdClientNotifDSServerAddrType.

Go Top

SECTION 3.7

Trap: cPsdClientDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PSDServerState	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The PSD $cPsdClientNotifDSServerAddress is down.	PSDServerState	CSG2
PSDServerState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The PSD $cPsdClientNotifDSServerAddress is up.	PSDServerState	CSG2

Description:

A notification of this type is generated when the PSD server goes DOWN. If the PSD client was in write/retrieving state, then that operation shall be be stopped.

Default Message:

$NodeDisplayName -- The PSD is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cPsdClientNotifDSServerAddrType	This object indicates the type of Internet address of the Data-Store server.
cPsdClientNotifDSServerAddress	This object specifies the Internet address of the Data-Store server . The type of address of an instance of this object is determined by the value of cPsdClientNotifDSServerAddrType.

Go Top

SECTION 3.8

Trap: ciscoContentServicesBMAStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BMAState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The BMA active_ccsBMAIpAddr:active_ccsBMAPort:active_ccsBMAVrfName is active.	BMAState	CSG2
BMAState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The BMA failed_ccsBMAIpAddr:failed_ccsBMAPort:failed_ccsBMAVrfName failed to respond to the CSG.	BMAState	CSG2
BMAState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- The CSG sent a node-alive request to BMA nawait_ccsBMAIpAddr:nawait_ccsBMAPort:nawait_ccsBMAVrfName and is waiting for a response.	BMAState	CSG2
					$NodeDisplayName -- The BMA standby_ccsBMAIpAddr:standby_ccsBMAPort:standby_ccsBMAVrfName is		

BMAState	Trap	Alarm	Yes	Informational	prepared to become active.	BMAState	CSG2
BMAState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The BMA suspended_ccsBMAIpAddr:suspended_ccsBMAPort:suspended_ccsBMAVrfName is suspended by the operator.	BMAState	CSG2
BMAState	Trap	Alarm	Yes	Informational	$NodeDisplayName -- The CSG sent an echo request to BMA echowait_ccsBMAIpAddr:echowait_ccsBMAPort:echowait_ccsBMAVrfName and is waiting for an echo response.	BMAState	CSG2
BMAState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The BMA $BMAIpAddr:$BMAPort:$BMAVrfName is active.	BMAState	CSG2
BMAState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The BMA $BMAIpAddr:$BMAPort:$BMAVrfName failed to respond to the CSG.	BMAState	CSG2
BMAState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- The CSG sent a node-alive request to BMA $BMAIpAddr:$BMAPort:$BMAVrfName and is waiting for a response.	BMAState	CSG2
BMAState	Poll	Alarm	Yes	Informational	$NodeDisplayName -- The BMA $BMAIpAddr:$BMAPort:$BMAVrfName is prepared to become active.	BMAState	CSG2
BMAState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The BMA $BMAIpAddr:$BMAPort:$BMAVrfName is suspended by the operator.	BMAState	CSG2
BMAState	Poll	Alarm	Yes	Informational	$NodeDisplayName -- The CSG sent an echo request to BMA $BMAIpAddr:$BMAPort:$BMAVrfName and is waiting for an echo response.	BMAState	CSG2

Description:

```
This notification is issued when ccsBMAStateChangeNotifEnabled        is set to 'true', and the billing mediation agent changes
state. There is one exception: No notification is issued
for state changes involving 'echowait' because this would
cause an excessive number of notifications.
```

Default Message:

$NodeDisplayName -- The BMA is active.
$NodeDisplayName -- BMA server failed to respond to the CSG.
$NodeDisplayName -- The CSG sent a node-alive request to this BMA and is waiting for a response.
$NodeDisplayName -- The BMA is prepared to become active.
$NodeDisplayName -- The BMA is suspended by the operator.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccsBMAState	States of a billing mediation agent. 'standby' - The server is prepared to become active. 'failed' - The server has failed to respond to requests. 'active' - The server has been activated to receive requests. 'echowait' - An echo request to this billing mediation agent and is waiting for a response. 'nawait' - A node-alive request to this billing mediation agent and is waiting for a response. 'suspended' - The server has receive a stop request from the operator.
ccsBMALostRecords	Total number of lost records since system initialization or the last time the counter wrapped.
ccsBMATotalSent	Total number of records sent to the billing mediation agent.
ccsBMAFailAck	Number of acknowledgments received from the billing mediation agent for which there are no outstanding requests.
ccsBMAOutstanding	Current number of messages waiting to be ACKed.

ccsBMAHighWater	The highest number of messages waiting for ACKs as reported by ccsBMAOutstanding object since object was reset as indicated by ccsBMAHighWaterResetTime. The only write operation allowed is to reset the value to 0.
ccsBMABadRecord	The number of bad records received. These are records in which an error was detected while attempting to decode the contents.
ccsBMARetransmit	The number of messages retransmitted to the billing mediation agent.

Operational Information:

- If the state of the BMA is 'Active' then no action is necessary

- If the state of the BMA is 'Stand By' then no action is necessary.This is an indication that a BMA instance had either started for the first time or had failed and the STANDBY server is ready to become Active. This must be followed by a state change to 'Active' for proper functioning.

- If the state of the BMA is 'Failed', it indicates that the BMA server has failed to respond to requests (either Echo Requests, Node Alive Requests, or Data Transfer Requests).

- If the state of a BMA is 'Echowait', it indicates that the CSG has sent an echo request to this BMA and is waiting for a response. CSG expects as reply an Echo Response message from the BMA. If the Echo Response is not received within 4 seconds, the Echo Request is resent to the BMA. “Resent” here means that the same packet is transmitted again containing the same information, sequence Number, etc. The CSG resends the Echo Request 3 times in case of no response from BMA. After the Echo Request has been sent 4 times without any reply (1st plus 3 repetitions), the CSG considers the BMA to be FAILED.

- If the state of the BMA is 'NAWAIT', it indicates that the CSG has sent a node-alive request to this BMA and is waiting for a response.CSG expects as reply a Node Alive Response message from the BMA. If the Node Alive Response is not received within 4 seconds, the Node Alive Request is resent to the server.“Resent”here means that the same packet is transmitted again containing same information, sequence Number, etc. The CSG resends the Node Alive Request 3 times in case of no response from server. After the Node Alive Request has been sent 4 times without any reply (1st plus 3 repetitions), the CSG considers the server to be FAILED. The CSG will send a new Node Alive Request message (new = new GTP’ Sequence Number) 60 seconds after the last non-responded Node Alive Request was sent, again resending 3 times if no response is received. CSG will keep resending every 60 seconds until a Node Alive response is received from the concerned server. Once a response is received from a server, the CSG will not send any other Node Alive Request to that server unless the CSG is restarted/reloaded.

- If the state of the BMA is 'SUSPENDED', it indicates that the server has received a stop request from the operator.

Troubleshooting:

If the status of the BMA shows as "Failed","NAWAIT" or "Echowait" there is a possibility of communication failure between the CSG and the BMA.There can be two possible reasons:

1. BMA server has crashed but the link between CSG and BMA is intact

If there are standby BMA servers deployed, the failure will be repaired automatically. The failure must be followed by a state change to 'standby' and ultimately to 'Active' corresponding to the standby BMA server assuming charge.However if there are no standby servers, follow to troubleshooting steps to ascertain this.

2. Link failure between CSG and BMA or Misconfiguration at CSG

If the link between the BMA and CSG fails or if there has been a wrong configuration at the CSG on how to find the BMA, there can be a transitions to these states.

Steps to Troubleshoot:

Step 1: Session into the CSG and ping the BMA.
Step 2: If ping is not successful, check routing table and CSG ARP for gateway to BMA.
Step 3: If ping is successful, run the show command : show ip csg bma detail.
Step 4: Observe counters “retransmits” and “failed acks” should increase.
Step 4: Turn on “debug ip csg gtp bma”, but be aware of the performance impact
Step 5: Check BMA status from the server side.
Step 6: Obtain a sniffer trace on all related vlans, analyze the trace and determine the faulty party.

Go Top

SECTION 3.9

Trap: ciscoDiaBaseProtPeerConnectionDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPeerConnectionState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	CSG2
DiameterPeerConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	CSG2
DiameterPeerConnectionState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	CSG2

DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	CSG2
DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	CSG2
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitConnAck.	DiameterPeerConnectionState	CSG2
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitICEA.	DiameterPeerConnectionState	CSG2
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is elect.	DiameterPeerConnectionState	CSG2
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitReturns.	DiameterPeerConnectionState	CSG2
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is closing.	DiameterPeerConnectionState	CSG2

Description:

```
An ciscoDiaBaseProtPeerConnectionDownNotif notification           is sent when both the following conditions are true:
1) the value of
ciscoDiaBaseProtEnablePeerConnectionDownNotif is true(1)
2) cdbpPeerStatsState changes to closed(1).
It can be utilized by an NMS to trigger logical/physical
entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The peer $cdbpPeerId state is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpLocalId	The implementation identification string for the Diameter software in use on the system, for example; 'diameterd'
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 3.10

Trap: ciscoDiaBaseProtPermanentFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPermanentFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol permanent failures for the diameter peer $cdbpPeerId has increased.	DiameterPermanentFailure	CSG2

Description:

```
An ciscoDiaBaseProtPermanentFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnablePermanentFailureNotif
   is true(1)
2) the value of cdbpPeerStatsPermanentFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol permanent failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsPermanentFailures	This object represents the Number of permanent failures returned to peer.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 3.11

Trap: ciscoDiaBaseProtProtocolErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterProtocolError	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol errors returned to the diameter peer $cdbpPeerId has increased.	DiameterProtocolError	CSG2

Description:

```
An ciscoDiaBaseProtProtocolErrorNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableProtocolErrorNotif
   is true(1)
2) the value of cdbpPeerStatsProtocolErrors changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol errors returned to the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsProtocolErrors	This object represents the Number of protocol errors returned to peer, but not including redirects.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 3.12

Trap: ciscoDiaBaseProtTransientFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterTransientFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol transient failures for the diameter peer $cdbpPeerId has increased.	DiameterTransientFailure	CSG2

Description:

```
An ciscoDiaBaseProtTransientFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableTransientFailureNotif
   is true(1)
2) the value of cdbpPeerStatsTransientFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol transient failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsTransientFailures	This object represents the transient failure count.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 3.13

Trap: ciscoMobilePolicyChargingControlPreloadError

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Gx-PreloadError	Trap	Alarm	No	Major	$NodeDisplayName -- A PCRF preloading error type $cmpccppsErrorState occurred.	Gx-PreloadError	CSG2

Description:

```
This notification is issued when cmpccPreloadErrorNotifEnabled       is set to true, and an error occurs in preloading as indicated
by the value of cmpccppsErrorState:
0   indicates PCRF has sent an incomplete Policy object.
1   indicates a mandatory AVP in the preloading message is
    missing.
2   indicates PCEF is not able to install/modify/remove a policy
    preloading object.
3   indicates PCRF sent the preloading objects in wrong order.
4   indicates PCRF tried to preload an object, which is already
    statically configured in PCEF.
255 indicates no error has occurred so far.
```

Default Message:

$NodeDisplayName -- A PCRF preloading error type $cmpccppsErrorState occurred.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cmpccppsErrorState	Specifies the error condition. 'preloadInconsistentData' indicates PCRF has sent an incomplete Policy object. 'preloadAVPMissing' indicates a mandatory AVP in the preloading message is missing.

	'preloadEnforceFailure' indicates PCEF is not able to install/modify/remove a policy preloading object. 'preloadWrongOrderFailure' indicates PCRF sent the preloading objects in wrong order. 'preloadStaticConfigConflict' indicates PCRF tried to preload an object, which is already statically configured in PCEF. 'preloadNoError' indicates no error has occurred so far. INTEGER is unknown
cmpccppsPreloadDataInconsistent	The number of times the preload data is inconsistent.
cmpccppsAVPMissing	The number of times the mandatory AVPs are missing.
cmpccppsEnforceFailures	The number of failures to enforce.
cmpccppsStaticConfigConflicts	The number of conflicts with static config.
cmpccppsWrongOrderFailures	The number of failures due to wrong order.
entPhysicalIndex	The index for this entry.

Go Top

SECTION 3.14

Trap: cmpccPreloadRollbackFailed

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Gx-RollbackFailed	Trap	Alarm	No	Major	$NodeDisplayName -- Object rollback failed on $entPhysicalName. Reason: $cmpccRollbackFailedReason	Gx-RollbackFailed	CSG2

Description:

```
This notification is generated when rollback of an object        fails, which indicates that object could be out of sync. The
cmpccppsRollbackFailedReason present in the varbind list,
indicates the reason that triggers the sending for
'cmpccPreloadRollbackFailed' notification. The entPhysicalName
identifies the entity that implements the PCEF functionality of
the Gx interface.
```

Default Message:

$NodeDisplayName -- Object rollback failed on $entPhysicalName. Reason: $cmpccRollbackFailedReason

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cmpccRollbackFailedReason	This object indicates the reason that triggers the sending for 'cmpccPreloadRollbackFailed' notification. When read, this object always returns the value 'none'. Other values are relevant when this object is used as a varbind in a notification. 'none' indicates no rollback failure has occurred. 'acctPolicyMap' indicates rollback for accounting policy-map has failed. 'contentPolicy' indicates rollback for content-policy has failed. 'serviceContent' indicates rollback for service-content has failed. 'billingService' indicates rollback for billing-service has failed. 'billingPlan' indicates rollback for billing-plan has failed. INTEGER is unknown
entPhysicalName	The textual name of the physical entity. The value of this

	object should be the name of the component as assigned by the local device and should be suitable for use in commands entered at the device's `console'. This might be a text name, such as `console' or a simple component number (e.g., port or module number), such as `1', depending on the physical component naming syntax of the device. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string. Note that the value of entPhysicalName for two physical entities will be the same in the event that the console interface does not distinguish between them, e.g., slot-1 and the card in slot-1.
entPhysicalIndex	The index for this entry.

Go Top

SECTION 3.15

Trap: cIscsiInstSessionFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-InstanceSessionState	Trap	Alarm	No	Warning	$NodeDisplayName - The active session has failed for the remote node - $cIscsiInstLastSsnRmtNodeName.	iSCSI-InstanceSessionState	CSG2

Description:

```
Sent when an active session is failed by either the initiator       or the target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The active session has failed for the remote node $cIscsiInstLastSsnRmtNodeName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiInstSsnFailures	This object counts the number of times a session belonging to this instance has been failed.
cIscsiInstLastSsnFailureType	The counter object in the cIscsiInstSsnErrorStatsTable that was incremented when the last session failure occurred. If the reason for failure is not found in the cIscsiInstSsnErrorStatsTable, the value { 0.0 } is used instead.
cIscsiInstLastSsnRmtNodeName	An octet string describing the name of the remote node from the failed session.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.

Go Top

SECTION 3.16

Trap: cIscsiIntrLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

iSCSI-InitiatorLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.	iSCSI-InitiatorLoginStatus	CSG2

Description:

```
Sent when a login is failed by a initiator.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiIntrLastTgtFailureAddrType	The type of Internet Network Address in cIscsiIntrLastTgtFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiIntrLoginFailures	This object counts the number of times a login attempt from this local initiator has failed.
cIscsiIntrLastFailureType	The type of the most recent failure of a login attempt from this initiator, represented as the OID of the counter object in cIscsiInitiatorLoginStatsTable for which the relevant instance was incremented. A value of 0.0

	indicates a type which is not represented by any of the counters in cIscsiInitiatorLoginStatsTable.
cIscsiIntrLastTgtFailureName	An octet string giving the name of the target that failed the last login attempt.
cIscsiIntrLastTgtFailureAddr	An Internet Network Address giving the host address of the target that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

SECTION 3.17

Trap: cIscsiTgtLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-TargetLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.	iSCSI-TargetLoginStatus	CSG2

Description:

```
Sent when a login is failed by a target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiTgtLastIntrFailureAddrType	The type of Internet Network Address in cIscsiTgtLastIntrFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be

	accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiTgtLoginFailures	This object counts the number of times a login attempt to this local target has failed.
cIscsiTgtLastFailureType	The type of the most recent failure of a login attempt to this target, represented as the OID of the counter object in cIscsiTargetLoginStatsTable for which the relevant instance was incremented. A value of 0.0 indicates a type which is not represented by any of the counters in cIscsiTargetLoginStatsTable.
cIscsiTgtLastIntrFailureName	An octet string giving the name of the initiator that failed the last login attempt.
cIscsiTgtLastIntrFailureAddr	An Internet Network Address giving the host address of the initiator that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

SECTION 3.18

Trap: ciscoTap2MediationTimedOut

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationTimedOut	Trap	Alarm	Yes	Normal	$NodeDisplayName - Tap2Mediation status is active.	Tap2MediationTimedOut	CSG2
Tap2MediationTimedOut	Trap	Alarm	Yes	Critical	$NodeDisplayName - Tap2Mediation status is notInService.	Tap2MediationTimedOut	CSG2
Tap2MediationTimedOut	Trap	Alarm	Yes	Warning	$NodeDisplayName - Tap2Mediation status is notReady.	Tap2MediationTimedOut	CSG2
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndGo.	Tap2MediationTimedOut	CSG2
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndWait.	Tap2MediationTimedOut	CSG2
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is destroy.	Tap2MediationTimedOut	CSG2

Description:

```
When an intercept is autonomously removed by an intercepting       device, such as due to the time specified in
cTap2MediationTimeout arriving, the device notifies the manager
of the action.
```

Default Message:

$NodeDisplayName - Tap2Mediation status is active.
$NodeDisplayName - Tap2Mediation status is notReady.
$NodeDisplayName - Tap2Mediation status is notInService.
$NodeDisplayName - Tap2Mediation status is createAndGo.
$NodeDisplayName - Tap2Mediation status is createAndWait.
$NodeDisplayName - Tap2Mediation status is destroy.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2MediationStatus	The status of this conceptual row. This object is used to manage creation, modification and deletion of rows in this table. cTap2MediationTimeout may be modified at any time (even while the row is active). But when the row is active, the other writable objects may not be modified without setting its value to 'notInService'. The entry may not be deleted or deactivated by setting its value to 'destroy' or 'notInService' if there is any associated entry in cTap2StreamTable. The RowStatus textual convention is used to manage the creation and deletion of conceptual rows, and is used as the value of the SYNTAX clause for the status column of a conceptual row (as described in Section 7.7.1 of [2].) The status column has six defined values: - `active', which indicates that the conceptual row is available for use by the managed device; - `notInService', which indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device (see NOTE below); - `notReady', which indicates that the conceptual row exists in the agent, but is missing information necessary in order to be available for use by the managed device; - `createAndGo', which is supplied by a management station wishing to create a new instance of a conceptual row and to have its status automatically set to active, making it available for use by the managed device; - `createAndWait', which is supplied by a management station wishing to create a new instance of a conceptual row (but not make it available for use by the managed device); and, - `destroy', which is supplied by a management station wishing to delete all of the instances associated with an existing conceptual row. Whereas five of the six values (all except `notReady') may be specified in a management protocol set operation, only three values will be returned in response to a management protocol retrieval operation: `notReady', `notInService' or `active'. That is, when queried, an existing conceptual row has only three states: it is either available for use by the managed device (the status column has value `active'); it is not available for use by the managed device, though the agent has sufficient information to make it so (the status column has value `notInService'); or, it is not available for use by the managed device, and an attempt to make it so would fail because the agent has insufficient information (the state column has value `notReady'). NOTE WELL This textual convention may be used for a MIB table, irrespective of whether the values of that table's conceptual rows are able to be modified while it is active, or whether its conceptual rows must be taken out of service in order to be modified. That is, it is the responsibility of the DESCRIPTION clause of the status column to specify whether the status column must not be `active' in order for the value of some other column of the same conceptual row to be modified. If such a specification is made, affected columns may be changed by an SNMP set PDU if the RowStatus would not be equal to `active' either immediately before or after processing the PDU. In other words, if the PDU also contained a varbind that would change the RowStatus value, the column in question may be changed if the RowStatus was not equal to `active' as the PDU was received, or if the varbind sets the status to a value

other than 'active'.
Also note that whenever any elements of a row exist, the
RowStatus column must also exist.
To summarize the effect of having a conceptual row with a
status column having a SYNTAX clause value of RowStatus,
consider the following state diagram:
STATE
+--------------+-----------+-------------+-------------
| A | B | C | D
| |status col.|status column|
|status column | is | is |status column
ACTION |does not exist| notReady | notInService| is active
--------------+--------------+-----------+-------------+-------------
set status |noError ->D|inconsist- |inconsistent-|inconsistent-
column to | or | entValue| Value| Value
createAndGo |inconsistent- | | |
| Value| | |
--------------+--------------+-----------+-------------+-------------
set status |noError see 1|inconsist- |inconsistent-|inconsistent-
column to | or | entValue| Value| Value
createAndWait |wrongValue | | |
--------------+--------------+-----------+-------------+-------------
set status |inconsistent- |inconsist- |noError |noError
column to | Value| entValue| |
active | | | |
| | or | |
| | | |
| |see 2 ->D| ->D| ->D
--------------+--------------+-----------+-------------+-------------
set status |inconsistent- |inconsist- |noError |noError ->C
column to | Value| entValue| |
notInService | | | |
| | or | | or
| | | |
| |see 3 ->C| ->C|wrongValue
--------------+--------------+-----------+-------------+-------------
set status |noError |noError |noError |noError
column to | | | |
destroy | ->A| ->A| ->A| ->A
--------------+--------------+-----------+-------------+-------------
set any other |see 4 |noError |noError |see 5
column to some| | | |
value | | see 1| ->C| ->D
--------------+--------------+-----------+-------------+-------------
(1) goto B or C, depending on information available to the
agent.
(2) if other variable bindings included in the same PDU,
provide values for all columns which are missing but
required, then return noError and goto D.
(3) if other variable bindings included in the same PDU,
provide values for all columns which are missing but
required, then return noError and goto C.
(4) at the discretion of the agent, the return value may be
either:
inconsistentName: because the agent does not choose to
create such an instance when the corresponding
RowStatus instance does not exist, or
inconsistentValue: if the supplied value is
inconsistent with the state of some other MIB object's
value, or
noError: because the agent chooses to create the
instance.
If noError is returned, then the instance of the status
column must also be created, and the new state is B or C,
depending on the information available to the agent. If
inconsistentName or inconsistentValue is returned, the row
remains in state A.
(5) depending on the MIB definition for the column/table,
either noError or inconsistentValue may be returned.
NOTE: Other processing of the set request may result in a
response other than noError being returned, e.g.,

wrongValue, noCreation, etc.

Conceptual Row Creation

There are four potential interactions when creating a conceptual row: selecting an instance-identifier which is not in use; creating the conceptual row; initializing any objects for which the agent does not supply a default; and, making the conceptual row available for use by the managed device.

Interaction 1: Selecting an Instance-Identifier

The algorithm used to select an instance-identifier varies for each conceptual row. In some cases, the instance-identifier is semantically significant, e.g., the destination address of a route, and a management station selects the instance-identifier according to the semantics. In other cases, the instance-identifier is used solely to distinguish conceptual rows, and a management station without specific knowledge of the conceptual row might examine the instances present in order to determine an unused instance-identifier. (This approach may be used, but it is often highly sub-optimal; however, it is also a questionable practice for a naive management station to attempt conceptual row creation.)

Alternately, the MIB module which defines the conceptual row might provide one or more objects which provide assistance in determining an unused instance-identifier. For example, if the conceptual row is indexed by an integer-value, then an object having an integer-valued SYNTAX clause might be defined for such a purpose, allowing a management station to issue a management protocol retrieval operation. In order to avoid unnecessary collisions between competing management stations, `adjacent' retrievals of this object should be different.

Finally, the management station could select a pseudo-random number to use as the index. In the event that this index was already in use and an inconsistentValue was returned in response to the management protocol set operation, the management station should simply select a new pseudo-random number and retry the operation.

A MIB designer should choose between the two latter algorithms based on the size of the table (and therefore the efficiency of each algorithm). For tables in which a large number of entries are expected, it is recommended that a MIB object be defined that returns an acceptable index for creation. For tables with small numbers of entries, it is recommended that the latter pseudo-random index mechanism be used.

Interaction 2: Creating the Conceptual Row

Once an unused instance-identifier has been selected, the management station determines if it wishes to create and activate the conceptual row in one transaction or in a negotiated set of interactions.

Interaction 2a: Creating and Activating the Conceptual Row

The management station must first determine the column requirements, i.e., it must determine those columns for which it must or must not provide values. Depending on the complexity of the table and the management station's knowledge of the agent's capabilities, this determination can be made locally by the management station. Alternately, the management station issues a management protocol get operation to examine all columns in the conceptual row that it wishes to create. In response, for each column, there are three possible outcomes:

- a value is returned, indicating that some other management station has already created this conceptual row. We return to interaction 1.
- the exception `noSuchInstance' is returned, indicating that the agent implements the object-type associated with this column, and that this column in at least one conceptual row would be accessible in the MIB view used by the retrieval were it to exist. For those columns to which the agent provides read-create access,

the `noSuchInstance' exception tells the management station that it should supply a value for this column when the conceptual row is to be created.
- the exception `noSuchObject' is returned, indicating that the agent does not implement the object-type associated with this column or that there is no conceptual row for which this column would be accessible in the MIB view used by the retrieval. As such, the management station can not issue any management protocol set operations to create an instance of this column.
Once the column requirements have been determined, a management protocol set operation is accordingly issued. This operation also sets the new instance of the status column to `createAndGo'.
When the agent processes the set operation, it verifies that it has sufficient information to make the conceptual row available for use by the managed device. The information available to the agent is provided by two sources: the management protocol set operation which creates the conceptual row, and, implementation-specific defaults supplied by the agent (note that an agent must provide implementation-specific defaults for at least those objects which it implements as read-only). If there is sufficient information available, then the conceptual row is created, a `noError' response is returned, the status column is set to `active', and no further interactions are necessary (i.e., interactions 3 and 4 are skipped). If there is insufficient information, then the conceptual row is not created, and the set operation fails with an error of `inconsistentValue'.
On this error, the management station can issue a management protocol retrieval operation to determine if this was because it failed to specify a value for a required column, or, because the selected instance of the status column already existed. In the latter case, we return to interaction 1. In the former case, the management station can re-issue the set operation with the additional information, or begin interaction 2 again using `createAndWait' in order to negotiate creation of the conceptual row.
NOTE WELL
Regardless of the method used to determine the column requirements, it is possible that the management station might deem a column necessary when, in fact, the agent will not allow that particular columnar instance to be created or written. In this case, the management protocol set operation will fail with an error such as `noCreation' or `notWritable'. In this case, the management station decides whether it needs to be able to set a value for that particular columnar instance. If not, the management station re-issues the management protocol set operation, but without setting a value for that particular columnar instance; otherwise, the management station aborts the row creation algorithm.
Interaction 2b: Negotiating the Creation of the Conceptual Row
The management station issues a management protocol set operation which sets the desired instance of the status column to `createAndWait'. If the agent is unwilling to process a request of this sort, the set operation fails with an error of `wrongValue'. (As a consequence, such an agent must be prepared to accept a single management protocol set operation, i.e., interaction 2a above, containing all of the columns indicated by its column requirements.) Otherwise, the conceptual row is created, a `noError' response is returned, and the status column is immediately set to either `notInService' or `notReady', depending on whether it has sufficient information to make the conceptual row available for use by the managed device. If there is sufficient information available, then the status column is set to

`notInService'; otherwise, if there is insufficient information, then the status column is set to `notReady'. Regardless, we proceed to interaction 3.

Interaction 3: Initializing non-defaulted Objects

The management station must now determine the column requirements. It issues a management protocol get operation to examine all columns in the created conceptual row. In the response, for each column, there are three possible outcomes:

- a value is returned, indicating that the agent implements the object-type associated with this column and had sufficient information to provide a value. For those columns to which the agent provides read-create access (and for which the agent allows their values to be changed after their creation), a value return tells the management station that it may issue additional management protocol set operations, if it desires, in order to change the value associated with this column.
- the exception `noSuchInstance' is returned, indicating that the agent implements the object-type associated with this column, and that this column in at least one conceptual row would be accessible in the MIB view used by the retrieval were it to exist. However, the agent does not have sufficient information to provide a value, and until a value is provided, the conceptual row may not be made available for use by the managed device. For those columns to which the agent provides read-create access, the `noSuchInstance' exception tells the management station that it must issue additional management protocol set operations, in order to provide a value associated with this column.
- the exception `noSuchObject' is returned, indicating that the agent does not implement the object-type associated with this column or that there is no conceptual row for which this column would be accessible in the MIB view used by the retrieval. As such, the management station can not issue any management protocol set operations to create an instance of this column.

If the value associated with the status column is `notReady', then the management station must first deal with all `noSuchInstance' columns, if any. Having done so, the value of the status column becomes `notInService', and we proceed to interaction 4.

Interaction 4: Making the Conceptual Row Available

Once the management station is satisfied with the values associated with the columns of the conceptual row, it issues a management protocol set operation to set the status column to `active'. If the agent has sufficient information to make the conceptual row available for use by the managed device, the management protocol set operation succeeds (a `noError' response is returned). Otherwise, the management protocol set operation fails with an error of `inconsistentValue'.

NOTE WELL

A conceptual row having a status column with value `notInService' or `notReady' is unavailable to the managed device. As such, it is possible for the managed device to create its own instances during the time between the management protocol set operation which sets the status column to `createAndWait' and the management protocol set operation which sets the status column to `active'. In this case, when the management protocol set operation is issued to set the status column to `active', the values held in the agent supersede those used by the managed device.

If the management station is prevented from setting the status column to `active' (e.g., due to management station or network failure) the conceptual row will be left in the `notInService' or `notReady' state, consuming resources indefinitely. The agent must detect conceptual rows that

	have been in either state for an abnormally long period of time and remove them. It is the responsibility of the DESCRIPTION clause of the status column to indicate what an abnormally long period of time would be. This period of time should be long enough to allow for human response time (including `think time') between the creation of the conceptual row and the setting of the status to `active'. In the absense of such information in the DESCRIPTION clause, it is suggested that this period be approximately 5 minutes in length. This removal action applies not only to newly-created rows, but also to previously active rows which are set to, and left in, the notInService state for a prolonged period exceeding that which is considered normal for such a conceptual row. Conceptual Row Suspension When a conceptual row is `active', the management station may issue a management protocol set operation which sets the instance of the status column to `notInService'. If the agent is unwilling to do so, the set operation fails with an error of `wrongValue'. Otherwise, the conceptual row is taken out of service, and a `noError' response is returned. It is the responsibility of the DESCRIPTION clause of the status column to indicate under what circumstances the status column should be taken out of service (e.g., in order for the value of some other column of the same conceptual row to be modified). Conceptual Row Deletion For deletion of conceptual rows, a management protocol set operation is issued which sets the instance of the status column to `destroy'. This request may be made regardless of the current value of the status column (e.g., it is possible to delete conceptual rows which are either `notReady', `notInService' or `active'.) If the operation succeeds, then all instances associated with the conceptual row are immediately removed.
cTap2MediationContentId	cTap2MediationContentId is a session identifier, from the intercept application's perspective, and a content identifier from the Mediation Device's perspective. The Mediation Device is responsible for making sure these are unique, although the SNMP RowStatus row creation process will help by not allowing it to create conflicting entries. Before creating a new entry, a value for this variable may be obtained by reading cTap2MediationNewIndex to reduce the probability of a value collision.

Go Top

SECTION 3.19

Trap: ciscoNtpGeneralConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with all NTP servers is lost	NtpConnectionState	CSG2
NtpConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with NTP server has been restored	NtpConnectionState	CSG2

Description:

```
This trap is sent when the device loses connectivity            to all NTP servers.
```

Default Message:

$NodeDisplayName - Connection with all NTP servers is lost.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 3.20

Trap: ciscoNtpHighPriorityConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with the high priority NTP server is failed	NtpHighPriorityConnectionState	CSG2
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with the high priority NTP server is restored	NtpHighPriorityConnectionState	CSG2

Description:

```
A failure to connect with an high priority NTP server (e.g. a server at the lowest stratum) is detected.
```

Default Message:

$NodeDisplayName - Connection with the high priority NTP server is failed

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpPeersPeerAddress	The IP address of the peer. When creating a new association, a value should be set either for this object or the corresponding instance of cntpPeersPeerName, before the row is made active.
cntpPeersAssocId	An integer value greater than 0 that uniquely identifies a peer with which the local NTP server is associated.

Go Top

SECTION 3.21

Trap: ciscoNtpSrvStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpServerStatus	Trap	Alarm	Yes	Indeterminate	$NodeDisplayName - The NTP server status is unknown	NtpServerStatus	CSG2
NtpServerStatus	Trap	Alarm	Yes	Critical	$NodeDisplayName - The NTP server is not running	NtpServerStatus	CSG2
NtpServerStatus	Trap	Alarm	Yes	Warning	$NodeDisplayName - The NTP server is not synchronized to any time source	NtpServerStatus	CSG2
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to its own local clock	NtpServerStatus	CSG2
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a local hardware refclock	NtpServerStatus	CSG2
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a remote NTP server	NtpServerStatus	CSG2

Description:

```
This notification is generated whenever the value of cntpSysSrvStatus changes.
```

Default Message:

$NodeDisplayName - The NTP server status is unknown
$NodeDisplayName - The NTP server is not running
$NodeDisplayName - The NTP server is not synchronized to any time source
$NodeDisplayName - The NTP server is synchronized to its own local clock
$NodeDisplayName - The NTP server is synchronized to a local hardware refclock
$NodeDisplayName - The NTP server is synchronized to a remote NTP server

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpSysSrvStatus	Current state of the NTP server with values coded as follows: 1: server status is unknown 2: server is not running 3: server is not synchronized to any time source 4: server is synchronized to its own local clock 5: server is synchronized to a local hardware refclock (e.g. GPS) 6: server is synchronized to a remote NTP server INTEGER is unknown

Go Top

---

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 3.22

Status: SystemTraffic

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SystemTraffic	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The system traffic threshold is Acceptable. Value $SystemTrafficValue	SystemTraffic	CSG2
SystemTraffic	Poll	Alarm	Yes	Major	$NodeDisplayName -- The system traffic threshold is Exceeded. Value $SystemTrafficValue	SystemTraffic	CSG2

Description:

Traffic meter value, i.e. the percentage of bandwidth utilization for the previous polling interval.

Default Message:

$NodeDisplayName -- The system traffic threshold is $SystemTrafficState. Value $SystemTrafficValue

Message Substitution Variables:

Node	Substitution variables for Node related data.
SystemTrafficState	Acceptable or Exceeded
SystemTrafficValue	The value of sysTraffic

Go Top

SECTION 3.23

Trap: ciscoTap2MIBActive

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MIBActive	Trap	Event	No	Informational	$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.	Tap2MIBActive	CSG2

Description:

```
This Notification is sent when an intercepting router or       switch is first capable of intercepting a packet corresponding
to a configured data stream. The value of the corresponding
cTap2StreamType which identifies the actual intercept stream
type is included in this notification.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.  Filter
installation can take a long period of time, during which call
progress may be delayed.
```

Default Message:

$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 3.24

Trap: ciscoTap2MediationDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .	Tap2MediationDebug	CSG2

Description:

```
When there is intervention needed due to some events related       to entries configured in cTap2MediationTable, the device
notifies the manager of the event.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.
```

Default Message:

$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 3.25

Trap: ciscoTap2StreamDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2StreamDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId	Tap2StreamDebug	CSG2

Description:

```
When there is intervention needed due to some events related        to entries configured in cTap2StreamTable, the device
notifies the manager of the event.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.
```

Default Message:

$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId.br>

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.
cTap2DebugStreamId	The value of this object is that of cTap2StreamIndex of an entry in cTap2StreamTable. This object along with cTap2DebugMediationId identifies an entry in cTap2StreamTable. The value of this object may be zero, in which this debug message is regarding a Mediation Device, but not a particular stream. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2StreamTable fails.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 3.26

Trap: ciscoTap2Switchover

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2Switchover	Trap	Event	No	Informational	$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.	Tap2Switchover	CSG2

Description:

```
This notification is sent when there is a redundant (standby)        route processor available on the intercepting device and the
current active processor is going down causing standby to
takeover. Note that this notification may be sent by the
intercepting device only when it had a chance to know before it
goes down.
Mediation device when received this notification should assume
that configured intercepts on the intercepting device no longer
exist, when the standby processor takes control. This means that
the Mediation device should again configure the intercepts.
```

Default Message:

$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 4.1

Trap: caemTemperatureNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
TemperatureStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported temperature state normal on $ciscoEnvMonTemperatureStatusDescr.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state critical on $ciscoEnvMonTemperatureStatusDescr.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state not functioning on $ciscoEnvMonTemperatureStatusDescr.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported temperature state not present on $ciscoEnvMonTemperatureStatusDescr.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported temperature state shutdown on $ciscoEnvMonTemperatureStatusDescr.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported temperature state warning on $ciscoEnvMonTemperatureStatusDescr.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state $ciscoEnvMonTemperatureState on $ciscoEnvMonTemperatureStatusDescr.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported temperature state normal on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state critical on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state not functioning on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported temperature state not present on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported temperature state shutdown on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported temperature state warning on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state $ciscoEnvMonTemperatureState on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported temperature state normal on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state critical on	TemperatureStateChange	Common

					$ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.		
TemperatureStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state not functioning on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported temperature state not present on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported temperature state shutdown on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported temperature state warning on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state $ciscoEnvMonTemperatureState on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName - Reported temperature state 'normal' on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName - Reported temperature state 'not present' on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName - Reported temperature state 'warning' on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state 'critical' on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state 'not functioning' on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Poll	Alarm	Yes	Critical	$NodeDisplayName - Reported temperature state 'shutdown' on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common
TemperatureStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported temperature state '$ciscoEnvMonTemperatureState' on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.	TemperatureStateChange	Common

Description:

A caemTemperatureNotification is sent if the over temperature condition is detected in the managed system. This is a replacement for the ciscoEnvMonTemperatureNotification trap because the information 'ciscoEnvMonTemperatureStatusValue' required by the trap is not available in the managed system.

Default Message:

$NodeDisplayName - Reported Temperature state $ciscoEnvMonTemperatureState on $ciscoEnvMonTemperatureStatusDescr.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ciscoEnvMonTemperatureStatusDescr	Textual description of the testpoint being instrumented. This description is a short textual label, suitable as a human-sensible identification for the rest of the information in the entry.
ciscoEnvMonTemperatureState	The current state of the testpoint being instrumented.

See Also:

ciscoEnvMonTemperatureNotification Trap

Go Top

SECTION 4.2

Trap: caemVoltageNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

VoltageStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported Voltage state normal on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported Voltage state critical on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported Voltage state not functioning on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported Voltage state not present on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported Voltage state shutdown on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported Voltage state warning on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported Voltage state $ciscoEnvMonVoltageState on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported voltage state normal on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported voltage state critical on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported voltage state not functioning on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported voltage state not present on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported voltage state shutdown on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported voltage state warning on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported voltage state $ciscoEnvMonVoltageState on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported voltage state normal on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported voltage state critical on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported voltage state not functioning on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported voltage state not present on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported voltage state shutdown on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported voltage state warning on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported voltage state $ciscoEnvMonVoltageState on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.	VoltageStateChange	Common
VoltageStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName - Reported Voltage state 'normal' on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName - Reported Voltage state 'not present' on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName - Reported Voltage state 'warning' on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported Voltage state 'critical' on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported Voltage state 'not functioning' on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Poll	Alarm	Yes	Critical	$NodeDisplayName - Reported Voltage state 'shutdown' on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common
VoltageStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported Voltage state '$ciscoEnvMonVoltageState' on $ciscoEnvMonVoltageStatusDescr.	VoltageStateChange	Common

Description:

A caemVoltageNotification is sent if the over voltage condition is detected and ciscoEnvMonVoltageState is not set to 'notPresent' in the managed system. This is a replacement for the ciscoEnvMonVoltageNotification trap because the information 'ciscoEnvMonVoltageStatusValue' required by the trap is not available in the managed system.

Default Message:

$NodeDisplayName - Reported Voltage state $ciscoEnvMonVoltageState on $ciscoEnvMonVoltageStatusDescr.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ciscoEnvMonVoltageStatusDescr	Textual description of the testpoint being instrumented. This description is a short textual label, suitable as a human-sensible identification for the rest of the information in the entry.
ciscoEnvMonVoltageState	The current state of the testpoint being instrumented.

See Also:

ciscoEnvMonVoltageNotification Trap

Go Top

SECTION 4.3

Trap: ciscoRFIssuStateNotifRev1

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RFIssuStatus	Trap	Alarm	No	Major	$NodeDisplayName - The State of the system is $RFIssuState. Switch Reason: $RFSwitchReason.	RFIssuStatus	Common

Description:

```
An ISSU notification to indicate the new state of       the system.
```

Default Message:

$NodeDisplayName - The State of the system is $RFIssuState. Switch Reason: $RFSwitchReason.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cRFStatusIssuStateRev1/RFIssuState	The current ISSU state of the system. ISSU state represents the current system state. init - This state represents the initial state of the system. The ISSU process is not running at this stage. The only CLI for ISSU process that can be executed in this state is the loadversion CLI. systemReset - If a system reset occurs, or the abortversion CLI is executed, the state of the system is pushed to this state. loadVersion - When the Standby signs in after the loadversion CLI is executed, the state of the system is changed to loadVersion. loadVersionSwitchover - If a switchover occurs in the loadVersion state, by the user, or because the Active crashes, the new state of the system will be loadVersionSwitchover. It is analogous to the runVersion state, except that the runversion CLI was not executed. runVersion - When the Standby signs in after executing the runversion CLI, the state of the system is changed

	to runVersion. runVersionSwitchover - if a switchover occurs while the system is in the runVersion state, the new state will be called runVersionSwitchover. It is analogous to the loadVersion state. commitVersion - When the Standby signs in after the commitversion CLI is executed, the state of the system is changed to commitVersion.
cRFStatusLastSwactReasonCode/RFSwitchReason	The reason for the last switch of activity. Reason codes for the switch of activity from an active redundant unit to its standby peer unit. unsupported - the 'reason code' is an unsupported feature none - no SWACT has occurred notKnown - reason is unknown userInitiated - a safe, manual SWACT was initiated by user userForced - a manual SWACT was forced by user; ignoring pre-conditions, warnings and safety checks activeUnitFailed - active unit failure caused an auto SWACT activeUnitRemoved - active unit removal caused an auto SWACT
cRFStatusIssuFromVersion/RFStatusIssuFromVersion	The IOS version from with the user is upgrading
cRFStatusIssuToVersion/RFStatusIssuToVersion	The IOS version to with the user is upgrading

Go Top

SECTION 4.4

Trap: casServerStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AAAServerState	Trap	Event	Yes	Normal	An AAA server is up on $NodeDisplayName.	AAAServerState	Common
AAAServerState	Trap	Event	Yes	Major	An AAA server is dead on $NodeDisplayName.	AAAServerState	Common
AAAServerState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- An AAA server $casAddress:$casAuthenPort-$casProtocol:$casAcctPort is up.	AAAServerState	Common
AAAServerState	Poll	Alarm	Yes	Major	$NodeDisplayName -- An AAA server $casAddress:$casAuthenPort-$casProtocol:$casAcctPort is dead.	AAAServerState	Common

Description:

An Authentication, Authorization and Accounting (AAA) server statechange notification is generated whenever an AAA server connection state changes value. An AAA server state may be either 'up' or 'dead'.

Default Message:

AAA server is $casState on $NodeDisplayName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
casState	A server is marked dead if it does not respond after maximum retransmissions. A server is marked up again either after a waiting period or if some response is received from it. The initial value of casState is 'up(1)' at system re-initialization. This will only transition to 'dead(2)'

	if an attempt to communicate fails.
casPreviousStateDuration	This object provides the elapsed time the server was been in its previous state prior to the most recent transition of casState.
casTotalDeadTime	The total elapsed time this server's casState has had the value 'dead(2)' since system re-initialization.

Operational Information:

- The object casState does not necessarily indicate the current state of the server. This is because casState is always up(1) unless an AAA request fails. In that case, casState is set to dead(2) and then reset to up(1) to allow the router to send requests to the server after a failure.
- The number of minutes casState remains dead(2) is specified by the command "radius-server deadtime *minutes*". For example, if server deadtime is 5 minutes and an AAA request fails, a trap is generated with casState set to dead(2). Five minutes later, another trap is generated with casState set to up(1) even though the server may still be down.

Diagnostic Commands:

1. To display information about AAA sessions as seen in the AAA Session MIB use

show aaa sessions

2. To display information about the number of packets sent to and receivedfrom AAA servers use

show aaa servers

Go Top

SECTION 4.5

Trap: entConfigChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EntityConfiguration	Trap	Alarm	No	Warning	An entity configuration change occurred on $NodeDisplayName.	EntityConfiguration	Common

Description:

An entConfigChange notification is generated when the value ofentLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls. An agent should not generate more than one entConfigChange 'notification-event' in a given time interval (five seconds is the suggested default). A 'notification-event' is the transmission of a single trap or inform PDU to a list of notification destinations. If additional configuration changes occur within the throttling period, then notification-events for these changes should be suppressed by the agent until the current throttling period expires. At the end of a throttling period, one notification-event should be generated if any configuration changes occurred since the start of the throttling period. In such a case, another throttling period is started right away. The NMS should periodically check the value of entLastChangeTime to detect any missed entConfigChange notification-events, e.g., due to throttling or transmission loss.

Default Message:

An entity configuration change occurred on $NodeDisplayName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router

	that sent the trap.

Operational Information:

- This trap can indicate the failure of a port adapter (PA) or error conditions on the PA that might affect the functionality of all interfaces and connected customers.
- If a port adapter was removed then you may want to replace the field replaceable unit.
- If a port adapter was added or operational status change occurred then no action is required.

Go Top

SECTION 4.6

Trap: risingAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RMONRising	Trap	Alarm	No	Warning	An RMON rising alarm (Index: $alarmIndex) occurred on $NodeDisplayName. ($alarmVariable=$alarmValue which is above threshold $alarmRisingThreshold.	RMONRising	Common

Description:

The SNMP trap that is generated when an alarm entry crosses itsrising threshold and generates an event that is configured for sending SNMP traps.

Default Message:

An RMON rising alarm (Index: $alarmIndex) occurred on $NodeDisplayName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
alarmIndex	An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.
alarmVariable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled. Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists that can restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is thus no acceptable means of restricting the read access that could be obtained through the alarm mechanism, the probe must only grant write access to this object in those views that have read access to all objects on the probe. During a set operation, if the supplied variable name is not available in the selected MIB view, a badValue error must be returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe must change the status of this alarmEntry to invalid(4).
alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If

	the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.
alarmValue	The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes.
alarmRisingThreshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3). After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.

Go Top

SECTION 4.7

Trap: fallingAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RMONFalling	Trap	Alarm	No	Warning	An RMON falling alarm (Index: $alarmIndex) occurred on $NodeDisplayName. ($alarmVariable=$alarmValue which is below threshold $alarmFallingThreshold.	RMONFalling	Common

Description:

The SNMP trap that is generated when an alarm entry crosses itsfalling threshold and generates an event that is configured for sending SNMP traps.

Default Message:

An RMON falling alarm (Index: $alarmIndex) occurred on $NodeDisplayName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
alarmIndex	An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.
alarmVariable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled. Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists that can restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is thus no acceptable means of restricting the read access that could be obtained through the alarm mechanism, the probe must only grant write access to this object in those views that have read access to all objects on the probe.

	During a set operation, if the supplied variable name is not available in the selected MIB view, a badValue error must be returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe must change the status of this alarmEntry to invalid(4).
alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.
alarmValue	The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes.
alarmFallingThreshold	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated. A single event will also be generated if the first sample after this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3). After a falling event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold.

Go Top

SECTION 4.8

Trap: ciscoFlashDeviceChangeTrap

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FlashDevice	Trap	Alarm	Yes	Warning	Flash device removed or inserted on $NodeDisplayName. Device name: $ciscoFlashDeviceName.	FlashDevice	Common
FlashDevice	Trap	Alarm	Yes	Normal	Flash device inserted on $NodeDisplayName. Device name: $ciscoFlashDeviceName.	FlashDevice	Common
FlashDevice	Trap	Alarm	Yes	Warning	Flash device removed on $NodeDisplayName. Device name: $ciscoFlashDeviceName.	FlashDevice	Common
FlashDevice	Trap	Alarm	Yes	Normal	Flash device inserted on $NodeDisplayName. Device name: $ciscoFlashDeviceNameExtended.	FlashDevice	Common
FlashDevice	Trap	Alarm	Yes	Warning	Flash device removed on $NodeDisplayName. Device name: $ciscoFlashDeviceNameExtended.	FlashDevice	Common

Description:

A ciscoFlashDeviceChangeTrap is sent whenever a removable Flashdevice is inserted or removed.

Default Message:

Flash device removed or inserted on $NodeDisplayName. Device name: $ciscoFlashDeviceName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
	This object will give the minimum partition size supported

ciscoFlashDeviceMinPartitionSize	for this device. For systems that execute code directly out of Flash, the minimum partition size needs to be the bank size. (Bank size is equal to the size of a chip multiplied by the width of the device. In most cases, the device width is 4 bytes, and so the bank size would be four times the size of a chip). This has to be so because all programming commands affect the operation of an entire chip (in our case, an entire bank because all operations are done on the entire width of the device) even though the actual command may be localized to a small portion of each chip. So when executing code out of Flash, one needs to be able to write and erase some portion of Flash without affecting the code execution. For systems that execute code out of DRAM or ROM, it is possible to partition Flash with a finer granularity (for eg., at erase sector boundaries) if the system code supports such granularity. This object will let a management entity know the minimum partition size as defined by the system. If the system does not support partitioning, the value will be equal to the device size in ciscoFlashDeviceSize. The maximum number of partitions that could be configured will be equal to the minimum of ciscoFlashDeviceMaxPartitions and (ciscoFlashDeviceSize / ciscoFlashDeviceMinPartitionSize).
ciscoFlashDeviceName	Flash device name. This name is used to refer to the device within the system. Flash operations get directed to a device based on this name. The system has a concept of a default device. This would be the primary or most used device in case of multiple devices. The system directs an operation to the default device whenever a device name is not specified. The device name is therefore mandatory except when the operation is being done on the default device, or, the system supports only a single Flash device. The device name will always be available for a removable device, even when the device has been removed.

Go Top

SECTION 4.9

Trap: cefcModuleStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ModuleStatus	Trap	Alarm	Yes	Normal	The module status of a field replaceable unit has changed to (ok) on $NodeDisplayName. Description: $entPhysicalDescr	ModuleStatus	Common
ModuleStatus	Trap	Alarm	Yes	Major	The module status of a field replaceable unit has changed to ($cefcModuleOperStatus) on $NodeDisplayName. Description: $entPhysicalDescr	ModuleStatus	Common
ModuleStatus	Poll	Alarm	Yes	Normal	$NodeDisplayName - the module status of replaceable unit '$entPhysicalName' has changed to 'ok'. Unit description: $entPhysicalDescr	ModuleStatus	Common
ModuleStatus	Poll	Alarm	Yes	Major	$NodeDisplayName - the module status of replaceable unit '$entPhysicalName' has changed to '$cefcModuleOperStatus'. Unit description: $entPhysicalDescr	ModuleStatus	Common

Description:

This notification is generated when the value ofcefcModuleOperStatus changes.It can be utilized by an NMS to update the status of the module it is managing.

Default Message:

The module status of a field replaceable unit has changed to ($cefcModuleOperStatus) on $NodeDisplayName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
	This object shows the module's operational state.

cefcModuleOperStatus	Operational module states. Valid values are : • unknown(1) - Module is not in one of other states normal operational states. • ok(2) - Module is operational. • disabled(3) - Module is administratively disabled. • okButDiagFailed(4) - Module is operational but there is some diagnostic information available. • boot(5) - Module is currently in the process of bringing up image. After boot, it starts its operational software and transitions to the appropriate state. • selfTest(6) - Module is performing selfTest. • failed(7) - Module has failed due to some condition not stated above. • missing(8) - Module has been provisioned, but it is missing • mismatchWithParent(9) - Module is not compatible with parent entity. Module has not been provisioned and wrong type of module is plugged in. This state can be cleared by plugging in the appropriate module. • mismatchConfig(10) - Module is not compatible with the current configuration.Module was correctly provisioned earlier, however the module was replaced by an incompatible module. This state can be resolved by clearing the configuration, or replacing with the appropriate module. • diagFailed(11) - Module diagnostic test failed due to some hardware failure. • dormant(12) - Module is waiting for an external or internal event to become operational • outOfServiceAdmin(13) - Module is administratively set to be powered on but out of service. • outOfServiceEnvTemp(14) - Module is powered on but out of service, due to environmental temperature problem. An out-of-service module consumes less power thus will cool down the board. • poweredDown(15) - Module is in powered down state. • poweredUp(16) - Module is in powered up state. • powerDenied(17) - System does not have enough power in power budget to power on this module. • powerCycled(18) - Module is being power cycled. • okButPowerOverWarning(19) - Module is drawing more power than allocated to this module. The module is still operational but may go into a failure state. This state may be caused by mis-configuration of power requirements (especially for inline power). • okButPowerOverCritical(20) - Module is drawing more power than this module is designed to handle. The module is still operational but may go into a failure state and could potentially take the system down. This state may be caused by gross mis-configuration of power requirements (especially for inline power).

	• syncInProgress(21) - Synchronization in progress. In a high availability system there will be 2 control modules, active and standby. This transitional state specifies the synchronization of data between the active and standby modules.
cefcModuleStatusLastChangeTime	The value of sysUpTime at the time the cefcModuleOperStatus is changed.

Operational Information:

- If Module is operational; no action is required.
- If a line card is provisioned for a slot but it is not present in the slot, insert a configured line card in the specific slot.
- You can enter the "show module" command to view error message details.

Diagnostic Commands:

1. To display status information about the module use the show module command in privileged EXEC mode.

show module [<1-6> | all | services | version]

<1-6>	(Optional) Module slot number
all	(Optional) Displays all linecard module information
services	(Optional) Displays dervices enabled on the linecard module
version	(Optional) Displays all linecard version information

2. To display information about the power status, use the show power command.

show power [{available | redundancy-mode | {status {all
| {module *slot*}}} | {power-supply *number*}
| total | used} | {inline [*interface number*]}]

available	(Optional) Displays the available system power (margin).
redundancy-mode	(Optional) Displays the power supply redundancy mode.
status	(Optional) Displays the power status.
all	Displays all the FRU types.
module *slot*	Displays the power status for a specific module.
power-supply *number*	Displays the power status for a specific power supply; valid values are 1 and 2.
total	(Optional) Displays the total power available from power supplies.
used	(Optional) Displays the total power budgeted for powered-on items.
inline	(Optional) Displays the inline power status.
interface number	(Optional) Specifies the interface type; possible valid values are ethernet, fastethernet, gigabitethernet, tengigabitethernet, null, port-channel, and vlan.

Go Top

SECTION 4.10

Trap: cefcPowerStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PowerStatus	Trap	Alarm	Yes	Normal	The power status of a field replaceable unit has changed to (on) on $NodeDisplayName. Description: $entPhysicalDescr	PowerStatus	Common
PowerStatus	Trap	Alarm	Yes	Major	The power status of a field replaceable unit has changed to ($cefcFRUPowerOperStatus) on $NodeDisplayName. Description: $entPhysicalDescr	PowerStatus	Common
PowerStatus	Poll	Alarm	Yes	Normal	$NodeDisplayName - the power status of replaceable unit '$entPhysicalName' has changed to 'on'. Unit description: $entPhysicalDescr	PowerStatus	Common
PowerStatus	Poll	Alarm	Yes	Major	$NodeDisplayName - the power status of replaceable unit '$entPhysicalName' has changed to '$cefcFRUPowerOperStatus'. Unit description: $entPhysicalDescr	PowerStatus	Common

Description:

The cefcFRUPowerStatusChange notificationindicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.

Default Message:

The power status of a field replaceable unit has changed to ($cefcFRUPowerOperStatus) on $NodeDisplayName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cefcFRUPowerOperStatus	Operational FRU Status types. valid values are: • offEnvOther(1) - FRU is powered off because of a problem not listed below. • on(2) - FRU is powered on. • offAdmin(3) - Administratively off. • offDenied(4) - FRU is powered off because available system power is insufficient. • offEnvPower(5) - FRU is powered off because of power problem in the FRU. for example, the FRU's power translation (DC-DC converter) or distribution failed. • offEnvTemp(6) - FRU is powered off because of temperature problem. • offEnvFan(7) - FRU is powered off because of fan problems. • failed(8) - FRU is in failed state. • onButFanFail(9) - FRU is on, but fan has failed. • offCooling(10) - FRU is powered off because of the system's insufficient cooling capacity. • offConnectorRating(11) - FRU is powered off because of the system's connector rating exceeded. • onButInlinePowerFail(12) - FRU is on, but no inline power is being delivered as the data/inline power component of the FRU has failed.
cefcFRUPowerAdminStatus	Administratively desired FRU power state types. Valid values are: • on(1) - Turn FRU on. • off(2) - Turn FRU off. Inline power means that the FRU itself won't cost any power but the external device connecting to the FRU will drain the power from FRU. For example, the IP phone device. The FRU is a port of a switch with voice ability and IP phone will cost power from the port once it connects to the port. • inlineAuto(3) - Turn FRU inline power to auto mode. It means that the FRU will try to detect whether the connecting device needs power or not. If it needs power, the FRU will supply power. If it doesn't, the FRU will treat the device as a regular network device. • inlineOn(4) - Turn FRU inline power to on mode. It means that once the device connects to the FRU, the FRU will always supply power to the device no matter the device needs the power or not. • powerCycle(5) - Power cycle the FRU. This value may be specified in a management protocol set operation, it will not be returned in response to a management protocol retrieval operation.

Operational Information:

- If FRU is powered on; no action is required.
- If FRU is administratively off; no action is required.
- If FRU is powered off because of an unknown problem or if is powered off because available system power is insufficient check the power usage.

Diagnostic Commands:

To display information about the power status, use the show power command.

show power [{available | redundancy-mode | {status {all | {module *slot*}}} | {power-supply *number*} | total | used} | {inline [*interface number*]}]

available	(Optional) Displays the available system power (margin).
redundancy-mode	(Optional) Displays the power supply redundancy mode.
status	(Optional) Displays the power status.
all	Displays all the FRU types.
module *slot*	Displays the power status for a specific module.
power-supply *number*	Displays the power status for a specific power supply; valid values are 1 and 2.
total	(Optional) Displays the total power available from power supplies.
used	(Optional) Displays the total power budgeted for powered-on items.
inline	(Optional) Displays the inline power status.
interface number	(Optional) Specifies the interface type; possible valid values are ethernet, fastethernet, gigabitethernet, tengigabitethernet, null, port-channel, and vlan.

Go Top

SECTION 4.11

Trap: rttMonNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPSLAReaction	Trap	Alarm	Yes	Normal	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - Reaction variable $rttMonReactVar = $rttMonReactValue, Rising threshold = $rttMonReactThresholdRising, Falling threshold = $rttMonReactThresholdFalling	IPSLAReaction	Common
IPSLAReaction	Trap	Alarm	Yes	Warning	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - Reaction variable $rttMonReactVar = $rttMonReactValue, Rising threshold = $rttMonReactThresholdRising, Falling threshold = $rttMonReactThresholdFalling	IPSLAReaction	Common

Description:

A rttMonNotification indicates the occurrence of a thresholdviolation, and it indicates the previous violation has subsided for a subsequent operation. When the RttMonRttType is 'pathEcho', this notification will only be sent when the threshold violation occurs during an operation to the target and not to a hop along the path to the target. This also applies to the subsiding of a threshold condition. If History is not being collected, the instance values for the rttMonHistoryCollectionAddress object will not be valid. When RttMonRttType is not 'echo' or 'pathEcho' the rttMonHistoryCollectionAddress object will be null. rttMonReactVar defines the type of reaction that is configured for the probe (e.g jitterAvg, rtt etc). In the rttMonReactTable there are trap definitions for the probes and each probe may have more than one trap definitions for various types (e.g rtt, jitterAvg, packetLoossSD etc). So the object rttMonReactVar indicates the type (e.g. rtt, packetLossSD, timeout etc) for which threshold violation traps has been generated. The object rttMonEchoAdminLSPSelector will be valid only for the probes based on 'mplsLspPingAppl' RttMonProtocol. For all

other probes it will be null.

Default Message:

$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - Reaction variable
$rttMonReactVar = $rttMonReactValue, Rising threshold =
$rttMonReactThresholdRising, Falling threshold =
$rttMonReactThresholdFalling

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
rttMonCtrlAdminTag	A string which is used by a managing application to identify the RTT target. This string is inserted into trap notifications, but has no other significance to the agent.
rttMonHistoryCollectionAddress	When the RttMonRttType is 'echo' or 'pathEcho' this is a string which specifies the address of the target for the this RTT operation. For all other values of RttMonRttType this string will be null. This address will be the address of the hop along the path to the rttMonEchoAdminTargetAddress address, including rttMonEchoAdminTargetAddress address, or just the rttMonEchoAdminTargetAddress address, when the path information is not collected. This behavior is defined by the rttMonCtrlAdminRttType object. The interpretation of this string depends on the type of RTT operation selected, as specified by the rttMonEchoAdminProtocol object. See rttMonEchoAdminTargetAddress for a complete description.
rttMonReactVar	This object specifies the type of reaction configured for a probe.The reaction types 'rtt', 'timeout', and 'connectionLoss' can be configured for all probe types.The reaction type 'verifyError' can be configured for all probe types except RTP probe type. The reaction types 'jitterSDAvg', 'jitterDSAvg', 'jitterAvg', 'packetLateArrival', 'packetOutOfSequence', 'maxOfPositiveSD', 'maxOfNegativeSD', 'maxOfPositiveDS' and 'maxOfNegativeDS' can be configured for UDP jitter and ICMP jitter probe types only. The reaction types 'mos' and 'icpif' can be configured for UDP jitter and ICMP jitter probe types only. The reaction types 'packetLossDS', 'packetLossSD' and 'packetMIA' can be configured for UDP jitter, and RTP probe types only. The reaction types 'iaJitterDS', 'frameLossDS', 'mosLQDS', 'mosCQDS', 'rFactorDS', 'iaJitterSD', 'rFactorSD', 'mosCQSD' can be configured for RTP probe type only. The reaction types 'successivePacketLoss', 'maxOfLatencyDS', 'maxOfLatencySD', 'latencyDSAvg', 'latencySDAvg' and 'packetLoss' can be configured for ICMP jitter probe type only.
rttMonReactOccurred	This object is set to true when the configured threshold condition is violated as defined by rttMonReactThresholdType. It will be again set to 'false' if the condition reverses. This object is set to true in the following conditions: - rttMonReactVar is set to timeout and rttMonCtrlOperTimeoutOccurred set to true. - rttMonReactVar is set to connectionLoss and rttMonCtrlOperConnectionLostOccurred set to true. - rttMonReactVar is set to verifyError and rttMonCtrlOperVerifyErrorOccurred is set to true. - For all other values of rttMonReactVar, if the corresponding value exceeds the configured rttMonReactThresholdRising. This object is set to false in the following conditions:

	- rttMonReactVar is set to timeout and rttMonCtrlOperTimeoutOccurred set to false. - rttMonReactVar is set to connectionLoss and rttMonCtrlOperConnectionLostOccurred set to false. - rttMonReactVar is set to verifyError and rttMonCtrlOperVerifyErrorOccurred is set to false. - For all other values of rttMonReactVar, if the corresponding value fall below the configured rttMonReactThresholdFalling. When the RttMonRttType is 'pathEcho' or 'pathJitter', this object is applied only to the rttMonEchoAdminTargetAddress and not to intermediate hops to the Target.
rttMonReactValue	This object will be set when the configured threshold condition is violated as defined by rttMonReactThresholdType and holds the actual value that violated the configured threshold values. This object is not valid for the following values of rttMonReactVar and It will be always 0: - timeout - connectionLoss - verifyError.
rttMonReactThresholdRising	This object defines the higher threshold limit. If the value (e.g rtt, jitterAvg, packetLossSD etc) rises above this limit and if the condition specified in rttMonReactThresholdType are satisfied, a trap is generated. Default value of rttMonReactThresholdRising for 'rtt' is 5000 'jitterAvg' is 100. 'jitterSDAvg' is 100. 'jitterDSAvg' 100. 'packetLossSD' is 10000. 'packetLossDS' is 10000. 'mos' is 500. 'icpif' is 93. 'packetMIA' is 10000. 'packetLateArrival' is 10000. 'packetOutOfSequence' is 10000. 'maxOfPositiveSD' is 10000. 'maxOfNegativeSD' is 10000. 'maxOfPositiveDS' is 10000. 'maxOfNegativeDS' is 10000. 'iaJitterDS' is 20. 'frameLossDS' is 10000. 'mosLQDS' is 400. 'mosCQDS' is 400. 'rFactorDS' is 80. 'successivePacketLoss' is 1000. 'maxOfLatencyDS' is 5000. 'maxOfLatencySD' is 5000. 'latencyDSAvg' is 5000.

	'latencySDAvg' is 5000. 'packetLoss' is 10000. This object is not applicable if the rttMonReactVar is 'timeout', 'connectionLoss' or 'verifyError'. For 'timeout', 'connectionLoss' and 'verifyError' default value of rttMonReactThresholdRising will be 0.
rttMonReactThresholdFalling	This object defines a lower threshold limit. If the value (e.g rtt, jitterAvg, packetLossSD etc) falls below this limit and if the conditions specified in rttMonReactThresholdType are satisfied, a trap is generated. Default value of rttMonReactThresholdFalling 'rtt' is 3000 'jitterAvg' is 100. 'jitterSDAvg' is 100. 'jitterDSAvg' 100. 'packetLossSD' is 10000. 'packetLossDS' is 10000. 'mos' is 500. 'icpif' is 93. 'packetMIA' is 10000. 'packetLateArrival' is 10000. 'packetOutOfSequence' is 10000. 'maxOfPositiveSD' is 10000. 'maxOfNegativeSD' is 10000. 'maxOfPositiveDS' is 10000. 'maxOfNegativeDS' is 10000. 'iaJitterDS' is 20. 'frameLossDS' is 10000. 'mosLQDS' is 310. 'mosCQDS' is 310. 'rFactorDS' is 60. 'successivePacketLoss' is 1000. 'maxOfLatencyDS' is 3000. 'maxOfLatencySD' is 3000. 'latencyDSAvg' is 3000. 'latencySDAvg' is 3000. 'packetLoss' is 10000. 'iaJitterSD' is 20. 'mosCQSD' is 310. 'rFactorSD' is 60. This object is not applicable if the rttMonReactVar is 'timeout', 'connectionLoss' or 'verifyError'. For

	'timeout', 'connectionLoss' and 'verifyError' default value of rttMonReactThresholdFalling will be 0.
rttMonEchoAdminLSPSelector	A string which specifies a valid 127/8 address. This address is of the form 127.x.y.z. This address is not used to route the MPLS echo packet to the destination but is used for load balancing in cases where the IP payload's destination address is used for load balancing.

Go Top

SECTION 4.12

Trap: rttMonLpdGrpStatusNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPSLAGroupStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - IP SLA Probe $rttMplsVpnMonCtrlTag - LPD group status is up for target $rttMonLpdGrpStatsTargetPE.	IPSLAGroupStatus	Common
IPSLAGroupStatus	Trap	Alarm	Yes	Warning	$NodeDisplayName - IP SLA Probe $rttMplsVpnMonCtrlTag - LPD group status is $rttMonLpdGrpStatsGroupStatus for target $rttMonLpdGrpStatsTargetPE.	IPSLAGroupStatus	Common

Description:

A rttMonLpdGrpStatusNotification indicates that the LPD Group statusrttMonLpdGrpStatsGroupStatus has changed indicating some connectivity change to the target PE. This has resulted in rttMonLpdGrpStatsGroupStatus changing value.

Default Message:

$NodeDisplayName - IP SLA Probe $rttMplsVpnMonCtrlTag - LPD group status is $rttMonLpdGrpStatsGroupStatus for target $rttMonLpdGrpStatsTargetPE.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
rttMplsVpnMonCtrlTag	A string which is used by a managing application to identify the RTT target. This string will be configured as rttMonCtrlAdminTag for all the operations configured by this Auto SAA L3 MPLS VPN. The usage of this value in Auto SAA L3 MPLS VPN is same as rttMonCtrlAdminTag in RTT operation.
rttMonLpdGrpStatsTargetPE	The object is a string that specifies the address of the target PE for this LPD group.
rttMonLpdGrpStatsGroupStatus	This object identifies the LPD Group status. When the LPD Group status changes and rttMplsVpnMonReactLpdNotifyType is set to 'lpdGroupStatus' or 'lpdAll' a rttMonLpdGrpStatusNotification will be generated. When the LPD Group status value is 'unknown' or changes to 'unknown' this notification will not be generated.When LSP Path Discovery is enabled for a particular row in rttMplsVpnMonCtrlTable, 'single probes' in the 'lspGroup' probe cannot generate notifications independently but will be generating depending on the state of the group. Notifications are only generated if the failure/restoration of an individual probe causes the state of the LPD Group to change. This object will be set to 'unknown' on reset.

Go Top

SECTION 4.13

Trap: rttMonTimeoutNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPSLATimeout	Trap	Alarm	Yes	Normal	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - RTT operation timeout cleared.	IPSLATimeout	Common
IPSLATimeout	Trap	Alarm	Yes	Warning	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - RTT operation timeout.	IPSLATimeout	Common

Description:

A rttMonTimeoutNotification indicates the occurrence of a timeoutfor a RTT operation, and it indicates the clearing of such a condition by a subsequent RTT operation. Precisely, this has resulted in rttMonCtrlOperTimeoutOccurred changing value. When the RttMonRttType is 'pathEcho', this notification will only be sent when the timeout occurs during an operation to the target and not to a hop along the path to the target. This also applies to the clearing of the timeout. If History is not being collected, the instance values for the rttMonHistoryCollectionAddress object will not be valid. When RttMonRttType is not 'echo' or 'pathEcho' the rttMonHistoryCollectionAddress object will be null.

This trap is currently deprecated.

Default Message:

$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - RTT operation timeout.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
rttMonCtrlAdminTag	A string which is used by a managing application to identify the RTT target. This string is inserted into trap notifications, but has no other significance to the agent.
rttMonHistoryCollectionAddress	When the RttMonRttType is 'echo' or 'pathEcho' this is a string which specifies the address of the target for the this RTT operation. For all other values of RttMonRttType this string will be null. This address will be the address of the hop along the path to the rttMonEchoAdminTargetAddress address, including rttMonEchoAdminTargetAddress address, or just the rttMonEchoAdminTargetAddress address, when the path information is not collected. This behavior is defined by the rttMonCtrlAdminRttType object. The interpretation of this string depends on the type of RTT operation selected, as specified by the rttMonEchoAdminProtocol object. See rttMonEchoAdminTargetAddress for a complete description.
rttMonCtrlOperTimeoutOccurred	This object will change its value for all RttMonRttTypes. This object is set to true when an operation times out, and set to false when an operation completes under rttMonCtrlAdminTimeout. When this value changes, a reaction may occur, as defined by rttMonReactAdminTimeoutEnable. When the RttMonRttType is 'pathEcho', this timeout applies only to the rttMonEchoAdminTargetAddress and not to intermediate hops to the Target. If a trap is sent it is a rttMonTimeoutNotification. When this value changes and any one of the rttMonReactTable row has rttMonReactVar object value as 'timeout(7)', a reaction may occur. If a trap is sent it is rttMonNotification with rttMonReactVar value of 'timeout'.

Go Top

Trap: rttMonThresholdNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPSLAOverThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - RTT operation threshold violation cleared.	IPSLAOverThreshold	Common
IPSLAOverThreshold	Trap	Alarm	Yes	Warning	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - RTT operation threshold violation.	IPSLAOverThreshold	Common

Description:

A rttMonThresholdNotification indicates the occurrence of athreshold violation for a RTT operation, and it indicates the previous violation has subsided for a subsequent RTT operation. Precisely, this has resulted in rttMonCtrlOperOverThresholdOccurred changing value. When the RttMonRttType is 'pathEcho', this notification will only be sent when the threshold violation occurs during an operation to the target and not to a hop along the path to the target. This also applies to the subsiding of a threshold condition. If History is not being collected, the instance values for the rttMonHistoryCollectionAddress object will not be valid. When RttMonRttType is not 'echo' or 'pathEcho' the rttMonHistoryCollectionAddress object will be null.

This trap is currently deprecated.

Default Message:

$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - RTT operation threshold violation cleared.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
rttMonCtrlAdminTag	A string which is used by a managing application to identify the RTT target. This string is inserted into trap notifications, but has no other significance to the agent.
rttMonHistoryCollectionAddress	When the RttMonRttType is 'echo' or 'pathEcho' this is a string which specifies the address of the target for the this RTT operation. For all other values of RttMonRttType this string will be null. This address will be the address of the hop along the path to the rttMonEchoAdminTargetAddress address, including rttMonEchoAdminTargetAddress address, or just the rttMonEchoAdminTargetAddress address, when the path information is not collected. This behavior is defined by the rttMonCtrlAdminRttType object. The interpretation of this string depends on the type of RTT operation selected, as specified by the rttMonEchoAdminProtocol object. See rttMonEchoAdminTargetAddress for a complete description.
rttMonCtrlOperOverThresholdOccurred	This object will change its value for all RttMonRttTypes. This object is changed by operation completion times over threshold, as defined by rttMonReactAdminThresholdType. When this value changes, a reaction may occur, as defined by rttMonReactAdminThresholdType. If a trap is sent it is a rttMonThresholdNotification. This object is set to true if the operation completion time exceeds the rttMonCtrlAdminThreshold and set to false when an operation completes under rttMonCtrlAdminThreshold. When this value changes, a reaction may occur, as defined by rttMonReactThresholdType. If a trap is sent it is rttMonNotification with rttMonReactVar value of 'rtt'.

Go Top

SECTION 4.15

Trap: rttMonVerifyErrorNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPSLADataCorruption	Trap	Alarm	Yes	Warning	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - RTT operation data corruption.	IPSLADataCorruption	Common
IPSLADataCorruption	Trap	Alarm	Yes	Normal	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - RTT operation data corruption cleared.	IPSLADataCorruption	Common

Description:

A rttMonVerifyErrorNotification indicates the occurrence of a datacorruption in an RTT operation.

This trap is currently deprecated.

Default Message:

$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - RTT operation data corruption.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
rttMonCtrlAdminTag	A string which is used by a managing application to identify the RTT target. This string is inserted into trap notifications, but has no other significance to the agent.
rttMonHistoryCollectionAddress	When the RttMonRttType is 'echo' or 'pathEcho' this is a string which specifies the address of the target for the this RTT operation. For all other values of RttMonRttType this string will be null. This address will be the address of the hop along the path to the rttMonEchoAdminTargetAddress address, including rttMonEchoAdminTargetAddress address, or just the rttMonEchoAdminTargetAddress address, when the path information is not collected. This behavior is defined by the rttMonCtrlAdminRttType object. The interpretation of this string depends on the type of RTT operation selected, as specified by the rttMonEchoAdminProtocol object. See rttMonEchoAdminTargetAddress for a complete description.
rttMonCtrlOperVerifyErrorOccurred	This object is true if rttMonCtrlAdminVerifyData is set to true and data corruption occurs.

Go Top

SECTION 4.16

Trap: rttMonLpdDiscoveryNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPSLADiscoveryFailed	Trap	Alarm	Yes	Normal	$NodeDisplayName - IP SLA Probe $rttMplsVpnMonCtrlTag - LSP path discovery to $rttMonLpdGrpStatsTargetPE succeeded.	IPSLADiscoveryFailed	Common
IPSLADiscoveryFailed	Trap	Alarm	Yes	Warning	$NodeDisplayName - IP SLA Probe $rttMplsVpnMonCtrlTag - LSP path discovery to $rttMonLpdGrpStatsTargetPE failed.	IPSLADiscoveryFailed	Common

Description:

A rttMonLpdDiscoveryNotification indicates that the LSP PathDiscovery to the target PE has failed, and it also indicates the clearing of such condition. Precisely this has resulted in rttMonLpdGrpStatsLPDFailOccurred changing value.When the rttMonLpdGrpStatsLPDFailOccurred is 'false', the instance value for rttMonLpdGrpStatsLPDFailCause is not valid.

Default Message:

$NodeDisplayName - IP SLA Probe $rttMplsVpnMonCtrlTag - LSP path discovery to $rttMonLpdGrpStatsTargetPE failed.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
rttMplsVpnMonCtrlTag	A string which is used by a managing application to identify the RTT target. This string will be configured as rttMonCtrlAdminTag for all the operations configured by this Auto SAA L3 MPLS VPN. The usage of this value in Auto SAA L3 MPLS VPN is same as rttMonCtrlAdminTag in RTT operation.
rttMonLpdGrpStatsTargetPE	The object is a string that specifies the address of the target PE for this LPD group.
rttMonLpdGrpStatsLPDFailCause	This object identifies the cause of failure for the LSP Path Discovery last attempted. It will be only valid if rttMonLpdGrpStatsLPDFailOccurred is set to true. This object will be set to 'unknown' on reset.
rttMonLpdGrpStatsLPDFailOccurred	This object is set to true when the LSP Path Discovery to the target PE i.e. rttMonLpdGrpStatsTargetPE fails, and set to false when the LSP Path Discovery succeeds. When this value changes and rttMplsVpnMonReactLpdNotifyType is set to 'lpdPathDiscovery' or 'lpdAll' a rttMonLpdDiscoveryNotification will be generated. This object will be set to 'FALSE' on reset.

Go Top

SECTION 4.17

Trap: rttMonConnectionChangeNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPSLAConnectionLost	Trap	Alarm	Yes	Normal	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - connection to a target has been restored.	IPSLAConnectionLost	Common
IPSLAConnectionLost	Trap	Alarm	Yes	Warning	$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - connection to a target has been lost.	IPSLAConnectionLost	Common

Description:

This notification is only valid when the RttMonRttType is 'echo' or'pathEcho'. A rttMonConnectionChangeNotification indicates that a connection to a target (not to a hop along the path to a target) has either failed on establishment or been lost and when reestablished. Precisely, this has resulted in rttMonCtrlOperConnectionLostOccurred changing value. If History is not being collected, the instance values for the rttMonHistoryCollectionAddress object will not be valid. When RttMonRttType is not 'echo' or 'pathEcho' the rttMonHistoryCollectionAddress object will be null.

This trap is currently deprecated.

Default Message:

$NodeDisplayName - IP SLA Probe $rttMonCtrlAdminTag - connection to a target has been restored.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
rttMonCtrlAdminTag	A string which is used by a managing application to identify the RTT target. This string is inserted into trap notifications, but has no other significance to the agent.
rttMonHistoryCollectionAddress	When the RttMonRttType is 'echo' or 'pathEcho' this is a string which specifies the address of the target for the this RTT operation. For all other values of RttMonRttType this string will be null. This address will be the address of the hop along the path to the rttMonEchoAdminTargetAddress address, including rttMonEchoAdminTargetAddress address, or just the rttMonEchoAdminTargetAddress address, when the path information is not collected. This behavior is defined by the rttMonCtrlAdminRttType object. The interpretation of this string depends on the type of RTT operation selected, as specified by the rttMonEchoAdminProtocol object. See rttMonEchoAdminTargetAddress for a complete description.
rttMonCtrlOperConnectionLostOccurred	This object will only change its value when the RttMonRttType is 'echo' or 'pathEcho'. This object is set to true when the RTT connection fails to be established or is lost, and set to false when a connection is reestablished. When the RttMonRttType is 'pathEcho', connection loss applies only to the rttMonEchoAdminTargetAddress and not to intermediate hops to the Target. When this value changes and rttMonReactAdminConnectionEnable is true, a reaction will occur. If a trap is sent it is a rttMonConnectionChangeNotification. When this value changes and any one of the rttMonReactTable row has rttMonReactVar object value as 'connectionLoss(8)', a reaction may occur. If a trap is sent it is rttMonNotification with rttMonReactVar value of 'connectionLoss'.

Go Top

SECTION 4.18

Trap: ciscoProducts and snmpTraps

Description:

The ciscoProducts and snmpTraps traps provide information when a cold or warm start is performed on a router or the state of a router interface changes.

- COLD_START - A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration may be altered.
- WARM_START - A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
- LINK_DOWN - A linkDown trap signifies a failure in one of the communication links represented in the router's configuration has occurred.
- LINK_UP - A linkUp trap signifies that one of the communication links represented in a router's configuration has come up.

Default Message:

- $NodeDisplayName ($NodeClliCode) - Cold Start. Reason: $Varbind1.
- $NodeDisplayName ($NodeClliCode) - Warm Start. Reason: $Varbind1.
- $NodeDisplayName ($NodeClliCode) - Interface $IfDescr down. Reason: $Reason.
- $NodeDisplayName ($NodeClliCode) - Interface $IfDescr up. Reason: $Reason.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtainedfrom the MWTM database based on the IP address of the router that sent the trap.
IfIndex	The index in the router's configuration of an interface that has changedstate, extracted from the trap PDU.
IfDescr	The description or name of an interface that has changed state, extractedfrom the trap PDU.
IfType	The type of interface that has changed state, extracted from the trapPDU.
IfAlias	The interface alias.
Reason	The reason for a state change, extracted from the trap PDU.

Operational Information:

- If the type of the trap is COLD_START this is an indication that the router has rebooted. You may want to investigate why. You can look for crash files on bootflash: or flash: file systems. It can also indicate a power on.
- If the type of the trap is WARM_START this is an indication that the SNMP agent on the router has restarted. You may want to investigate why. It can indicate a software reload.
- If the type of the trap is LINK_DOWN this is an indication that an interface on the router has become unavailable. This may be due to an administrative action or a failure. It can also indicate an internal software error. You may want to investigate why.
- If the type of the trap is LINK_UP this is an indication that an interface has become available. No action is necessary.
- For LINK_UP and LINK_DOWN traps the Reason variable may have a value of "nosuchInstance". This is caused by the fact that not all interface types support inclusion in the SNMP MIB for the local interface table. When this value is encountered no reason for the state change is known.

Diagnostic Commands:

For LINK_DOWN trap use following commands to determine if the problem islocal to the device.

1. show cs7 mtp2 [congestion | state | statistics] *interface*

congestion	(Optional) Displays MTP2 congestion status.
state	(Optional) Displays MTP2 state machine status.
statistics	(Optional) Displays link statistics.
interface	(Optional) Serial Interface number.

2. show interfaces *interface* [stats | summary]

interface	Serial Interface number. Example Serial0/0:0
stats	(Optional) Displays interface packets & octets, in & out, by switching path
summary	(Optional) Displays interface summary

See Also:

AuthenticationFailure Trap

Go Top

SECTION 4.19

Trap: ciscoProducts and snmpTraps

Description:

The ciscoProducts and snmpTraps traps provide information when a cold or warm start is performed on a router or the state of a router interface changes.

- COLD_START - A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration may be altered.
- WARM_START - A warmStart trap signifies that the SNMPv2 entity, acting

in an agent role, is reinitializing itself such that its configuration is unaltered.

- LINK_DOWN - A linkDown trap signifies a failure in one of the communication links represented in the router's configuration has occurred.
- LINK_UP - A linkUp trap signifies that one of the communication links represented in a router's configuration has come up.

Default Message:

- $NodeDisplayName ($NodeCliCode) - Cold Start. Reason: $Varbind1.
- $NodeDisplayName ($NodeCliCode) - Warm Start. Reason: $Varbind1.
- $NodeDisplayName ($NodeCliCode) - Interface $IfDescr down. Reason: $Reason.
- $NodeDisplayName ($NodeCliCode) - Interface $IfDescr up. Reason: $Reason.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtainedfrom the MWTM database based on the IP address of the router that sent the trap.
IfIndex	The index in the router's configuration of an interface that has changedstate, extracted from the trap PDU.
IfDescr	The description or name of an interface that has changed state, extractedfrom the trap PDU.
IfType	The type of interface that has changed state, extracted from the trapPDU.
IfAlias	The interface alias.
Reason	The reason for a state change, extracted from the trap PDU.

Operational Information:

- If the type of the trap is COLD_START this is an indication that the router has rebooted. You may want to investigate why. You can look for crash files on bootflash: or flash: file systems. It can also indicate a power on.
- If the type of the trap is WARM_START this is an indication that the SNMP agent on the router has restarted. You may want to investigate why. It can indicate a software reload.
- If the type of the trap is LINK_DOWN this is an indication that an interface on the router has become unavailable. This may be due to an administrative action or a failure. It can also indicate an internal software error. You may want to investigate why.
- If the type of the trap is LINK_UP this is an indication that an interface has become available. No action is necessary.
- For LINK_UP and LINK_DOWN traps the Reason variable may have a value of "nosuchInstance". This is caused by the fact that not all interface types support inclusion in the SNMP MIB for the local interface table. When this value is encountered no reason for the state change is known.

Diagnostic Commands:

For LINK_DOWN trap use following commands to determine if the problem islocal to the device.

1. show cs7 mtp2 [congestion | state | statistics] *interface*

congestion	(Optional) Displays MTP2 congestion status.
state	(Optional) Displays MTP2 state machine status.
statistics	(Optional) Displays link statistics.
interface	(Optional) Serial Interface number.

2. show interfaces *interface* [stats | summary]

interface	Serial Interface number. Example Serial0/0:0
stats	(Optional) Displays interface packets & octets, in & out, by switching path
summary	(Optional) Displays interface summary

See Also:

AuthenticationFailure Trap

SECTION 4.20

Trap:ciscoSlbVirtualStateChange

Status:SlbVirtualStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SlbVirtualServerStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName -- SLB Virtual Server outOfService_slbEntity:outOfService_slbVirtualServerName -- This virtual server is not active and is not affecting client traffic.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName -- SLB Virtual Server inService_slbEntity:inService_slbVirtualServerName -- This virtual server is active and is load-balancing client traffic to available real servers.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server standby_slbEntity:standby_slbVirtualServerName -- This virtual server is in standby mode and is acting as a backup for a virtual server on another SLB device.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server inOperReal_slbEntity:inOperReal_slbVirtualServerName -- The real server associated with this redirect virtual server is not operational.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server stbInOperReal_slbEntity:stbInOperReal_slbVirtualServerName -- The real server associated with this virtual server is not operational and this virtual server is in standby state.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server testReal_slbEntity:testReal_slbVirtualServerName -- The real server associated with this virtual server is being tested.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server outOfMemory_slbEntity:outOfMemory_slbVirtualServerName -- This virtual server is not enabled because it does not have enough memory to hold the configured matching policy information.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName -- SLB Virtual Server $slbEntity:$slbVirtualServerName -- This virtual server is not active and is not affecting client traffic.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName -- SLB Virtual Server $slbEntity:$slbVirtualServerName -- This virtual server is active and is load-balancing client traffic to available real servers.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server $slbEntity:$slbVirtualServerName -- This virtual server is in standby mode and is acting as a backup for a virtual server on another SLB device.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server $slbEntity:$slbVirtualServerName -- The real server associated with this redirect virtual server is not operational.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server $slbEntity:$slbVirtualServerName --The real server associated with this virtual server is not operational and this virtual server is in standby state.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server $slbEntity:$slbVirtualServerName -- The real server associated with this virtual server is being tested.	SlbVirtualServerStateChange	Common
SlbVirtualServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Virtual Server $slbEntity:$slbVirtualServerName -- This virtual server is not enabled because it does not have enough memory to hold the configured matching policy information.	SlbVirtualServerStateChange	Common

Description:

This event is created when a virtual server changes to a new state.

Default Message:

$NodeDisplayName -- SLB Virtual Server
$slbEntity:$slbVirtualServerName -- This virtual server is not
active and is not affecting client traffic.
$NodeDisplayName -- SLB Virtual Server

$slbEntity:$slbVirtualServerName -- This virtual server is active and is load-balancing client traffic to available real servers.
$NodeDisplayName -- SLB Virtual Server
$slbEntity:$slbVirtualServerName -- This virtual server is in standby mode and is acting as a backup for a virtual server on another SLB device.
$NodeDisplayName -- SLB Virtual Server
$slbEntity:$slbVirtualServerName -- The real server associated with this redirect virtual server is not operational.
$NodeDisplayName -- SLB Virtual Server
$slbEntity:$slbVirtualServerName --The real server associated with this virtual server is not operational and this virtual server is in standby state.
$NodeDisplayName -- SLB Virtual Server
$slbEntity:$slbVirtualServerName -- The real server associated with this virtual server is being tested.
$NodeDisplayName -- SLB Virtual Server
$slbEntity:$slbVirtualServerName -- This virtual server is not enabled because it does not have enough memory to hold the configured matching policy information.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
slbVirtualServerState	The state of virtual server.
slbEntity	The SLB instance reference number for this server. This allows multiple SLB's to exist on the same SNMP system. This object's value generally corresponds to the slot number where the module resides.
slbVirtualServerName	The name of the virtual server.

Go Top

SECTION 4.21

Trap:ciscoSlbRealStateChange

Status: SlbRealStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SlbRealServerStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName -- SLB Real Server outOfService_slbEntity:outOfService_slbRealServerFarmName:outOfService_slbRealIpAddress:outOfService_slbRealPort -- This real server is out of service and is not in use as a destination for client connections.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName -- SLB Real Server inService_slbEntity:inService_slbRealServerFarmName:inService_slbRealIpAddress:inService_slbRealPort -- This real server is in service and is a destination for SLB client connections.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName -- SLB Real Server failed_slbEntity:failed_slbRealServerFarmName:failed_slbRealIpAddress:failed_slbRealPort -- This real server has failed.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server readyToTest_slbEntity:readyToTest_slbRealServerFarmName:readyToTest_slbRealIpAddress:readyToTest_slbRealPort -- This server has received a test probe from the SLB.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server testing_slbEntity:testing_slbRealServerFarmName:testing_slbRealIpAddress:testing_slbRealPort -- This server has failed and been given a test connection.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server maxConnsThrottle_slbEntity:maxConnsThrottle_slbRealServerFarmName:maxConnsThrottle_slbRealIpAddress:maxConnsThrottle_slbRealPort -- This real server has reached its maximum number of connections.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server maxClientsThrottle_slbEntity:maxClientsThrottle_slbRealServerFarmName:maxClientsThrottle_slbRealIpAddress:maxClientsThrottle_slbRealPort -- This real server has reached its maximum number of clients.	SlbRealServerStateChange	Common

SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server dfpThrottle_slbEntity:dfpThrottle_slbRealServerFarmName:dfpThrottle_slbRealIpAddress:dfpThrottle_slbRealPort -- DFP has lowered the weight of this server to throttle level, so that no new connections will be assigned to it until DFP raises its weight.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server probeFailed_slbEntity:probeFailed_slbRealServerFarmName:probeFailed_slbRealIpAddress:probeFailed_slbRealPort -- The probe to this server has failed. No new connections will be assigned to this server until a probe to this server succeeds.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server probeTesting_slbEntity:probeTesting_slbRealServerFarmName:probeTesting_slbRealIpAddress:probeTesting_slbRealPort -- This server has received a test probe from the SLB.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server operWait_slbEntity:operWait_slbRealServerFarmName:operWait_slbRealIpAddress:operWait_slbRealPort -- This real server is ready to go operational, but is waiting for the associated virtual server to be in service.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server testWait_slbEntity:testWait_slbRealServerFarmName:testWait_slbRealIpAddress:testWait_slbRealPort -- This server is ready to be tested. This state is applicable only when the server is used for http redirect load balancing.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server inbandProbeFailed_slbEntity:inbandProbeFailed_slbRealServerFarmName:inbandProbeFailed_slbRealIpAddress:inbandProbeFailed_slbRealPort -- This real server has failed the inband health probe agent.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server returnCodeFailed_slbEntity:returnCodeFailed_slbRealServerFarmName:returnCodeFailed_slbRealIpAddress:returnCodeFailed_slbRealPort -- This server has been disabled because it returned an HTTP code that matched a configured value.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This real server is out of service and is not in use as a destination for client connections.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This real server is in service and is a destination for SLB client connections.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This real server has failed.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This server has received a test probe from the SLB.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This server has failed and been given a test connection.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This real server has reached its maximum number of connections.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This real server has reached its maximum number of clients.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- DFP has lowered the weight of this server to throttle level, so that no new connections will be assigned to it until DFP raises its weight.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- The probe to this server has failed. No new connections will be assigned to this server until a probe to this server succeeds.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This server has received a test probe from the SLB.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This real server is ready to go operational, but is waiting for the associated virtual server to be in service.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This server is ready to be tested. This state is applicable only when the server is used for http redirect load balancing.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This real server has failed the inband health probe agent.	SlbRealServerStateChange	Common
SlbRealServerStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Real Server $slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- This server has been disabled because it returned an HTTP code that matched a configured value.	SlbRealServerStateChange	Common

Description:

This event occurrs when a real server
style="font-family: monospace;"> changes to a new state. The
value of slbRealServerState
indicates the new state.

Default Message:

$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This real server is out of service and is not in use as a destination

for client connections.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This real server is in service and is a destination for SLB client
connections.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This real server has failed.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This server has received a test probe from the SLB.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This server has failed and been given a test connection.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This real server has reached its maximum number of connections.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This real server has reached its maximum number of clients.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- DFP
has lowered the weight of this server to throttle level, so that no new
connections will be assigned to it until DFP raises its weight.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort -- The
probe to this server has failed. No new connections will be
assigned to this server until a probe to this server succeeds.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This server has received a test probe from the SLB.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This real server is ready to go operational, but is waiting for the
associated virtual server to be in service.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This server is ready to be tested. This state is applicable only when
the server is used for http redirect load balancing.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This real server has failed the inband health probe agent.
$NodeDisplayName -- SLB Real Server
$slbEntity:$slbRealServerFarmName:$slbRealIpAddress:$slbRealPort --
This server has been disabled because it returned an HTTP code that
matched a configured value.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
slbRealState	The current state of real server.
slbEntity	The SLB instance reference number for this server. This allows multiple SLB's to exist on the same SNMP system. This object's value generally corresponds to the slot number where the module resides.
slbRealServerFarmName	The real server's server farm name.
slbRealIpAddress	The IP address of real server.
slbRealPort	The TCP or UDP port of real server. This is used if SLB NAT is configured (see slbServerFarmNat). If SLB is not using NAT, this value will be 0.

Go Top

Trap:cslbxFtStateChange

Status:SlbFtStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SlbFaultToleranceStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName -- SLB Entity: notConfigFT_slbEntity -- SLB fault tolerance is not configured.	SlbFaultToleranceStateChange	Common
SlbFaultToleranceStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName -- SLB Entity: initializingFT_slbEntity -- SLB fault tolerance is initializing.	SlbFaultToleranceStateChange	Common
SlbFaultToleranceStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName -- SLB Entity: activeFT_slbEntity -- SLB fault tolerance is active.	SlbFaultToleranceStateChange	Common
SlbFaultToleranceStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName -- SLB Entity: standbyFT_slbEntity -- SLB fault tolerance is in standby mode.	SlbFaultToleranceStateChange	Common
SlbFaultToleranceStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName -- SLB Entity: $slbEntity -- SLB fault tolerance is not configured.	SlbFaultToleranceStateChange	Common
SlbFaultToleranceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName -- SLB Entity: $slbEntity -- SLB fault tolerance is initializing.	SlbFaultToleranceStateChange	Common
SlbFaultToleranceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName -- SLB Entity: $slbEntity -- SLB fault tolerance is active.	SlbFaultToleranceStateChange	Common
SlbFaultToleranceStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName -- SLB Entity: $slbEntity -- SLB fault tolerance is in standby mode.	SlbFaultToleranceStateChange	Common

Description:

The notification generated when the Fault Tolerance process changes to a new state.

Default Message:

$NodeDisplayName -- SLB Entity: $slbEntity -- SLB fault tolerance is not configured.
$NodeDisplayName -- SLB Entity: $slbEntity -- SLB fault tolerance is initializing.
$NodeDisplayName -- SLB Entity: $slbEntity -- SLB fault tolerance is active.
$NodeDisplayName -- SLB Entity: $slbEntity -- SLB fault tolerance is in standby mode.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cslbxFtState	The current Fault Tolerance state of this SLB device.
slbEntity	The SLB instance reference number for this server. This allows multiple SLB's to exist on the same SNMP system. This object's value generally corresponds to the slot number where the module resides.

Go Top

SECTION 4.23

Trap: moduleDown

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ModuleStatusState	Trap	Alarm	Yes	Major	$NodeDisplayName -- Module type $moduleType at index $moduleIndex is not ok.	ModuleStatusState	Common
ModuleStatusState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Module type $moduleType at index $moduleIndex is ok.	ModuleStatusState	Common

ModuleStatusState	Poll	Alarm	Yes	Indeterminate	$NodeDisplayName - The status of module $moduleTypeDescription at index $moduleIndex is undetermined.	ModuleStatusState	Common
ModuleStatusState	Poll	Alarm	Yes	Normal	$NodeDisplayName - The status of module $moduleTypeDescription at index $moduleIndex is normal.	ModuleStatusState	Common
ModuleStatusState	Poll	Alarm	Yes	Minor	$NodeDisplayName - module $moduleTypeDescription at index $moduleIndex has a minor fault.	ModuleStatusState	Common
ModuleStatusState	Poll	Alarm	Yes	Major	$NodeDisplayName - module $moduleTypeDescription at index $moduleIndex has a major fault.	ModuleStatusState	Common

Description:

A moduleDown trap signifies that the agent entity has detected that the moduleStatus object in this
MIB has transitioned out of the ok(2) state for
one of its modules.
The generation of this trap can be controlled by
the sysEnableModuleTraps object in this MIB.

Default Message:

$NodeDisplayName -- Module type $moduleType at index $moduleIndex is not ok.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
moduleIndex	A unique value for each module within the chassis.
moduleType	The type of module.

Operational Information:

- This trap can indicate many things. The module may not be compatible with the current configuration. Module can be in the powered down state or has a hardware failure. You can check the system logs for reasons of failure.

Diagnostic Commands:

To display status information about the module use the show module command in privileged EXEC mode.

show module [<1-6> | all | services | version]

<1-6>	(Optional) Module slot number
all	(Optional) Displays all linecard module information
services	(Optional) Displays devices enabled on the linecard module
version	(Optional) Displays all linecard version information

Go Top

SECTION 4.24

Trap: ciscoICsuDsuT1LoopStatusNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LOS	Trap	Event	Yes	Critical	$NodeDisplayName -- (LOS) Unable to detect the DS1 signal. Index=lossofSignal[2]	LOS	Common
LOS	Trap	Event	Yes	Normal	$NodeDisplayName -- (LOS cleared) Able to detect the DS1 signal. Index=lossofSignalCleared[2]	LOS	Common
LOS	Poll	Alarm	Yes	Normal	$NodeDisplayName $ifDescr (LOS cleared) Able to detect the DS1 signal.	LOS	Common
LOS	Poll	Alarm	Yes	Critical	$NodeDisplayName $ifDescr (LOS) Unable to detect the DS1 signal.	LOS	Common

Description:

```
Indicates a change in T1 Loop Status.
```

Default Message:

$NodeDisplayName -- (AIS, blue alarm) Indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (AIS, blue alarm cleared) The transmission interruption has cleared. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm) The transmitting equipment has lost its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm cleared) The transmitting equipment has recovered its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF) Unable to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF cleared) Able to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- Line placed in loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- Line taken out of loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS) Unable to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS cleared) Able to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
ciscoICsuDsuT1LoopStatus	Current Loop status of T1 CSU/DSU. Represented as a sum of a bit map. The variable bit positions are: 1 - lossofSignal (LOS); unable to detect the DS1 signal. 2 - lossofFrame (LOF); unable to synchronize on the DS1 signal. 4 - detectedRemoteAlarmIndication (RAI); indicates that the transmitting equipment has lost its incoming signal. RAI is commonly called yellow alarm. 8 - detectedAlarmIndicationSignal (AIS); indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Indicated by an unframed, all-'ones' signal. Also known as blue alarm. 16 - placedInLoopback; Line placed in loopback from remote.

Go Top

SECTION 4.25

Trap: ciscoICsuDsuT1LoopStatusNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LOF	Trap	Event	Yes	Critical	$NodeDisplayName -- (LOF) Unable to synchronize on the DS1 signal. Index=lossofFrame[2]	LOF	Common
LOF	Trap	Event	Yes	Normal	$NodeDisplayName -- (LOF cleared) Able to synchronize on the DS1 signal. Index=lossofFrameCleared[2]	LOF	Common
LOF	Poll	Alarm	Yes	Normal	$NodeDisplayName $ifDescr (LOF cleared) Able to synchronize on the DS1 signal.	LOF	Common
LOF	Poll	Alarm	Yes	Critical	$NodeDisplayName $ifDescr (LOF) Unable to synchronize on the DS1 signal.	LOF	Common

Description:

Indicates a change in T1 Loop Status.

Default Message:

$NodeDisplayName -- (AIS, blue alarm) Indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (AIS, blue alarm cleared) The transmission interruption has cleared. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm) The transmitting equipment has lost its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm cleared) The transmitting equipment has recovered its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF) Unable to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF cleared) Able to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- Line placed in loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- Line taken out of loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS) Unable to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS cleared) Able to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
ciscoICsuDsuT1LoopStatus	Current Loop status of T1 CSU/DSU. Represented as a sum of a bit map. The variable bit positions are: 1 - lossofSignal (LOS); unable to detect the DS1 signal. 2 - lossofFrame (LOF); unable to synchronize on the DS1 signal. 4 - detectedRemoteAlarmIndication (RAI); indicates that the transmitting equipment has lost its incoming signal. RAI is commonly called yellow alarm. 8 - detectedAlarmIndicationSignal (AIS); indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Indicated by an unframed, all-'ones' signal. Also known as blue alarm. 16 - placedInLoopback; Line placed in loopback from remote.

Go Top

SECTION 4.26

Trap: ciscoICsuDsuT1LoopStatusNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RAI	Trap	Event	Yes	Major	$NodeDisplayName -- (RAI, yellow alarm) The transmitting equipment has lost its incoming signal. Index=detectedRemoteAlarmIndication[2]	RAI	Common
RAI	Trap	Event	Yes	Normal	$NodeDisplayName -- (RAI, yellow alarm cleared) The transmitting equipment has recovered its incoming signal. Index=detectedRemoteAlarmIndicationCleared[2]	RAI	Common
RAI	Poll	Alarm	Yes	Normal	$NodeDisplayName $ifDescr (RAI, yellow alarm cleared) The transmitting equipment has recovered its incoming signal.	RAI	Common
RAI	Poll	Alarm	Yes	Major	$NodeDisplayName $ifDescr (RAI, yellow alarm) The transmitting equipment has lost its incoming signal.	RAI	Common

Description:

Indicates a change in T1 Loop Status.

Default Message:

$NodeDisplayName -- (AIS, blue alarm) Indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (AIS, blue alarm cleared) The transmission interruption has cleared. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm) The transmitting equipment has lost its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm cleared) The transmitting equipment has recovered its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF) Unable to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF cleared) Able to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- Line placed in loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- Line taken out of loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS) Unable to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS cleared) Able to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
ciscoICsuDsuT1LoopStatus	Current Loop status of T1 CSU/DSU. Represented as a sum of a bit map. The variable bit positions are: 1 - lossofSignal (LOS); unable to detect the DS1 signal. 2 - lossofFrame (LOF); unable to synchronize on the DS1 signal. 4 - detectedRemoteAlarmIndication (RAI); indicates that the

	transmitting equipment has lost its incoming signal. RAI is commonly called yellow alarm. 8 - detectedAlarmIndicationSignal (AIS); indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Indicated by an unframed, all-'ones' signal. Also known as blue alarm. 16 - placedInLoopback; Line placed in loopback from remote.

Go Top

SECTION 4.27

Trap: ciscoICsuDsuT1LoopStatusNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AIS	Trap	Event	Yes	Major	$NodeDisplayName -- (AIS, blue alarm) Indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Index=detectedAlarmIndicationSignal[2]	AIS	Common
AIS	Trap	Event	Yes	Normal	$NodeDisplayName -- (AIS, blue alarm cleared) The transmission interruption has cleared. Index=detectedAlarmIndicationSignalCleared[2]	AIS	Common
AIS	Poll	Alarm	Yes	Normal	$NodeDisplayName $ifDescr (AIS, blue alarm cleared) The transmission interruption has cleared.	AIS	Common
AIS	Poll	Alarm	Yes	Major	$NodeDisplayName $ifDescr (AIS, blue alarm) Indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment.	AIS	Common

Description:

```
Indicates a change in T1 Loop Status.
```

Default Message:

$NodeDisplayName -- (AIS, blue alarm) Indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (AIS, blue alarm cleared) The transmission interruption has cleared. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm) The transmitting equipment has lost its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm cleared) The transmitting equipment has recovered its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF) Unable to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF cleared) Able to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- Line placed in loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- Line taken out of loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS) Unable to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS cleared) Able to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
ciscoICsuDsuT1LoopStatus	Current Loop status of T1 CSU/DSU. Represented as a sum of a bit map. The variable bit positions are: 1 - lossofSignal (LOS); unable to detect the DS1 signal. 2 - lossofFrame (LOF); unable to synchronize on the DS1 signal. 4 - detectedRemoteAlarmIndication (RAI); indicates that the transmitting equipment has lost its incoming signal. RAI is commonly called yellow alarm. 8 - detectedAlarmIndicationSignal (AIS); indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Indicated by an unframed, all-'ones' signal. Also known as blue alarm. 16 - placedInLoopback; Line placed in loopback from remote.

Go Top

Trap: ciscoEnvMon

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ShutdownAlarm	Trap	Alarm	No	Critical	$NodeDisplayName - Shutting down due to environmental problems.	ShutdownAlarm	Common

Description:

The ciscoEnvMon traps provide information when the environmentalmonitoring subsystem on a Cisco router detects an error in the state of one of the environmental test points. These test points can include voltage, temperature, fans, and power supplies.

- ciscoEnvMonShutdownNotification - This trap is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown. This notification contains no objects so that it may be encoded and sent in the shortest amount of time possible. Even so, management applications should not rely on receiving such a notification as it may not be sent before the shutdown completes. The remaining ciscoEnvMon traps are usually generated before the shutdown state is reached, and as such they can convey more data and have a better chance of being sent than does the ciscoEnvMonShutdownNotification.
- ciscoEnvMonVoltageNotification - This trap is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage). (Deprecated)
- ciscoEnvMonTemperatureNotification - This trap is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage). (Deprecated)
- ciscoEnvMonFanNotification - This trap is sent if any one of the fans in the fan array (where extant) fails. (Deprecated)
- ciscoEnvMonRedundantSupplyNotification - This trap is sent if the redundant power supply (where extant) fails. (Deprecated)
- ciscoEnvMonVoltStatusChangeNotif - This trap is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage).
- ciscoEnvMonTempStatusChangeNotif - This trap is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage).
- ciscoEnvMonFanStatusChangeNotif - This trap is sent if any one of the fans in the fan array (where extant) fails.
- ciscoEnvMonSuppStatusChangeNotif - This trap is sent if the redundant power supply (where extant) fails.

Default Message:

- $NodeDisplayName - Shutting down due to environmental problems.
- $NodeDisplayName - Reported fan state $ciscoEnvMonFanState on $ciscoEnvMonFanStatusDescr.
- $NodeDisplayName - Reported power supply state $ciscoEnvMonSupplyState on $ciscoEnvMonSupplyStatusDescr.
- $NodeDisplayName - Reported temperature state $ciscoEnvMonTemperatureState on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.
- $NodeDisplayName - Reported voltage state $ciscoEnvMonVoltageState on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.

Message Substitution Variables:

Common	Substitution variables common to all traps.
	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
ciscoEnvMonFanState ciscoEnvMonSupplyState ciscoEnvMonTemperatureState ciscoEnvMonVoltageState	One of the following states: • Normal: the environment is good, such as low temperature. • Warning: the environment is bad, such as temperature above normal operation range but not too high. • Critical: the environment is very bad, such as temperature much higher than normal operation limit. • Shutdown: the environment is the worst, the system should be shutdown immediately. • NotPresent: the environmental monitor is not present, such as temperature sensors do not exist. • NotFunctioning: the environmental monitor does not function properly, such that a temperature sensor generates abnormal data like 1000 C.
ciscoEnvMonFanStatusDescr ciscoEnvMonSupplyStatusDescr ciscoEnvMonTemperatureStatusDescr ciscoEnvMonVoltageStatusDescr	The environmental test point being monitored.
ciscoEnvMonVoltageStatusValue	The current voltage measurement of the testpoint being instrumented.
ciscoEnvMonTemperatureStatusValue	The current temperature measurement of the testpoint being instrumented.

Operational Information:

- ciscoEnvMonShutdownNotification - Indicates an environment failure. Successive notifications can indicate the failing component. You can check the logs to collect additional information about the failure.
- ciscoEnvMonTemperatureNotification, ciscoEnvMonTempStatusChangeNotif - Indicates problems with cooling fans within device or rise in external temperature. If temperatures continue to rise device may fail.
- ciscoEnvMonVoltageNotification, ciscoEnvMonVoltStatusChangeNotif - Indicates problems with power supply. If voltage remains out of range replacement of related components may be required.
- ciscoEnvMonFanNotification, ciscoEnvMonFanStatusChangeNotif - Indicates failure of main fan or fans for power supply. You may want to check fans for obstruction of air flow or replace the system fan tray.
- ciscoEnvMonRedundantSupplyNotification, ciscoEnvMonSuppStatusChangeNotif - Indicates that a failure has occurred in the power supply. The backup power unit will provide power to device temporarily; but the failing device will need to be replaced to provide redundancy power supply. You can also try to reduce the system power consumption.
- You may want to notify your hardware support personnel of the problem.

Diagnostic Commands:

To display system status information "show environment" command inprivileged EXEC mode.

show environment [alarm | cooling | status | temperature |voltage]

alarm	(Optional) Displays environmental alarms. • status - Displays alarm status. • thresholds - Displays alarm thresholds
cooling	(Optional) Displays fan tray status, chassis cooling capacity, ambient temperature, and per-slot cooling capacity.
status	(Optional) Displays FRU operational status with power and temperature information.
temperature	(Optional) Displays FRU temperature information.
voltage	(Optional) Displays FRU voltage information.

Go Top

SECTION 4.29

Trap: ciscoEnvMon

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SupplyStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported power supply state normal on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported power supply state critical on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported power supply state not functioning on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported power supply state not present on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported power supply state shutdown on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported power supply state warning on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported power supply state $ciscoEnvMonSupplyState on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported power supply state normal on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported power supply state critical on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported power supply state not functioning on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported power supply state not present on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported power supply state shutdown on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported power supply state warning on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported power supply state $ciscoEnvMonSupplyState on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName - Reported Supply state 'normal' on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName - Reported Supply state 'not present' on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName - Reported Supply state 'warning' on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported Supply state 'critical' on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported Supply state 'not functioning' on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Poll	Alarm	Yes	Critical	$NodeDisplayName - Reported Supply state 'shutdown' on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common
SupplyStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported Supply state '$ciscoEnvMonSupplyState' on $ciscoEnvMonSupplyStatusDescr.	SupplyStateChange	Common

Description:

The ciscoEnvMon traps provide information when the environmentalmonitoring subsystem on a Cisco router detects an error in the state of one of the environmental test points. These test points can include voltage, temperature, fans, and power supplies.

- ciscoEnvMonShutdownNotification - This trap is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown. This notification contains no objects so that it may be encoded and sent in the shortest amount of time possible. Even so, management applications should not rely on receiving such a notification as it may not be sent before the shutdown completes. The remaining ciscoEnvMon traps are usually generated before the shutdown state is reached, and as such they can convey more data and have a better chance of being sent than does the ciscoEnvMonShutdownNotification.
- ciscoEnvMonVoltageNotification - This trap is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage). (Deprecated)
- ciscoEnvMonTemperatureNotification - This trap is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage). (Deprecated)
- ciscoEnvMonFanNotification - This trap is sent if any one of the

fans in the fan array (where extant) fails. (Deprecated)
- ciscoEnvMonRedundantSupplyNotification - This trap is sent if the redundant power supply (where extant) fails. (Deprecated)
- ciscoEnvMonVoltStatusChangeNotif - This trap is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage).
- ciscoEnvMonTempStatusChangeNotif - This trap is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage).
- ciscoEnvMonFanStatusChangeNotif - This trap is sent if any one of the fans in the fan array (where extant) fails.
- ciscoEnvMonSuppStatusChangeNotif - This trap is sent if the redundant power supply (where extant) fails.

Default Message:

- $NodeDisplayName - Shutting down due to environmental problems.
- $NodeDisplayName - Reported fan state $ciscoEnvMonFanState on $ciscoEnvMonFanStatusDescr.
- $NodeDisplayName - Reported power supply state $ciscoEnvMonSupplyState on $ciscoEnvMonSupplyStatusDescr.
- $NodeDisplayName - Reported temperature state $ciscoEnvMonTemperatureState on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.
- $NodeDisplayName - Reported voltage state $ciscoEnvMonVoltageState on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ciscoEnvMonFanState ciscoEnvMonSupplyState ciscoEnvMonTemperatureState ciscoEnvMonVoltageState	One of the following states: • Normal: the environment is good, such as low temperature. • Warning: the environment is bad, such as temperature above normal operation range but not too high. • Critical: the environment is very bad, such as temperature much higher than normal operation limit. • Shutdown: the environment is the worst, the system should be shutdown immediately. • NotPresent: the environmental monitor is not present, such as temperature sensors do not exist. • NotFunctioning: the environmental monitor does not function properly, such that a temperature sensor generates abnormal data like 1000 C.
ciscoEnvMonFanStatusDescr ciscoEnvMonSupplyStatusDescr ciscoEnvMonTemperatureStatusDescr ciscoEnvMonVoltageStatusDescr	The environmental test point being monitored.
ciscoEnvMonVoltageStatusValue	The current voltage measurement of the testpoint being instrumented.
ciscoEnvMonTemperatureStatusValue	The current temperature measurement of the testpoint being instrumented.

Operational Information:

- ciscoEnvMonShutdownNotification - Indicates an environment failure. Successive notifications can indicate the failing component. You can check the logs to collect additional information about the failure.

ciscoEnvMonTemperatureNotification, ciscoEnvMonTempStatusChangeNotif - Indicates problems with cooling fans within device or rise in external temperature. If temperatures continue to rise device may fail.

- ciscoEnvMonVoltageNotification, ciscoEnvMonVoltStatusChangeNotif - Indicates problems with power supply. If voltage remains out of range replacement of related components may be required.
- ciscoEnvMonFanNotification, ciscoEnvMonFanStatusChangeNotif - Indicates failure of main fan or fans for power supply. You may want to check fans for obstruction of air flow or replace the system fan tray.
- ciscoEnvMonRedundantSupplyNotification, ciscoEnvMonSuppStatusChangeNotif - Indicates that a failure has occurred in the power supply. The backup power unit will provide power to device temporarily; but the failing device will need to be replaced to provide redundancy power supply. You can also try to reduce the system power consumption.
- You may want to notify your hardware support personnel of the problem.

Diagnostic Commands:

To display system status information "show environment" command inprivileged EXEC mode.

show environment [alarm | cooling | status | temperature |voltage]

alarm	(Optional) Displays environmental alarms. • status - Displays alarm status. • thresholds - Displays alarm thresholds
cooling	(Optional) Displays fan tray status, chassis cooling capacity, ambient temperature, and per-slot cooling capacity.
status	(Optional) Displays FRU operational status with power and temperature information.
temperature	(Optional) Displays FRU temperature information.
voltage	(Optional) Displays FRU voltage information.

Go Top

SECTION 4.30

Trap: ciscoEnvMon

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FanStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported fan state normal on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported fan state critical on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported fan state not functioning on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported fan state not present on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported fan state shutdown on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported fan state warning on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported fan state $ciscoEnvMonFanState on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported fan state normal on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported fan state critical on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported fan state not functioning on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - Reported fan state not present on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Reported fan state shutdown on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Warning	$NodeDisplayName - Reported fan state warning on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Trap	Alarm	Yes	Major	$NodeDisplayName - Reported fan state $ciscoEnvMonFanState on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName - Reported Fan state 'normal' on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName - Reported Fan state 'not present' on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common

FanStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName - Reported Fan state 'warning' on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported Fan state 'critical' on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported Fan state 'not functioning' on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Poll	Alarm	Yes	Critical	$NodeDisplayName - Reported Fan state 'shutdown' on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common
FanStateChange	Poll	Alarm	Yes	Major	$NodeDisplayName - Reported Fan state '$ciscoEnvMonFanState' on $ciscoEnvMonFanStatusDescr.	FanStateChange	Common

Description:

The ciscoEnvMon traps provide information when the environmentalmonitoring subsystem on a Cisco router detects an error in the state of one of the environmental test points. These test points can include voltage, temperature, fans, and power supplies.

- ciscoEnvMonShutdownNotification - This trap is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown. This notification contains no objects so that it may be encoded and sent in the shortest amount of time possible. Even so, management applications should not rely on receiving such a notification as it may not be sent before the shutdown completes. The remaining ciscoEnvMon traps are usually generated before the shutdown state is reached, and as such they can convey more data and have a better chance of being sent than does the ciscoEnvMonShutdownNotification.
- ciscoEnvMonVoltageNotification - This trap is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage). (Deprecated)
- ciscoEnvMonTemperatureNotification - This trap is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage). (Deprecated)
- ciscoEnvMonFanNotification - This trap is sent if any one of the fans in the fan array (where extant) fails. (Deprecated)
- ciscoEnvMonRedundantSupplyNotification - This trap is sent if the redundant power supply (where extant) fails. (Deprecated)
- ciscoEnvMonVoltStatusChangeNotif - This trap is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage).
- ciscoEnvMonTempStatusChangeNotif - This trap is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the Warning, Critical, or Shutdown stage).
- ciscoEnvMonFanStatusChangeNotif - This trap is sent if any one of the fans in the fan array (where extant) fails.
- ciscoEnvMonSuppStatusChangeNotif - This trap is sent if the redundant power supply (where extant) fails.

Default Message:

- $NodeDisplayName - Shutting down due to environmental problems.
- $NodeDisplayName - Reported fan state $ciscoEnvMonFanState on $ciscoEnvMonFanStatusDescr.
- $NodeDisplayName - Reported power supply state $ciscoEnvMonSupplyState on $ciscoEnvMonSupplyStatusDescr.
- $NodeDisplayName - Reported temperature state $ciscoEnvMonTemperatureState on $ciscoEnvMonTemperatureStatusDescr. $ciscoEnvMonTemperatureStatusValue degrees.
- $NodeDisplayName - Reported voltage state $ciscoEnvMonVoltageState on $ciscoEnvMonVoltageStatusDescr. $ciscoEnvMonVoltageStatusValue millivolts.

Message Substitution Variables:

Common	Substitution variables common to all traps.
	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
ciscoEnvMonFanState ciscoEnvMonSupplyState ciscoEnvMonTemperatureState ciscoEnvMonVoltageState	One of the following states: • Normal: the environment is good, such as low temperature. • Warning: the environment is bad, such as temperature above normal operation range but not too high. • Critical: the environment is very bad, such as temperature much higher than normal operation limit. • Shutdown: the environment is the worst, the system should be shutdown immediately. • NotPresent: the environmental monitor is not present, such as temperature sensors do not exist. • NotFunctioning: the environmental monitor does not function properly, such that a temperature sensor generates abnormal data like 1000 C.
ciscoEnvMonFanStatusDescr ciscoEnvMonSupplyStatusDescr ciscoEnvMonTemperatureStatusDescr ciscoEnvMonVoltageStatusDescr	The environmental test point being monitored.
ciscoEnvMonVoltageStatusValue	The current voltage measurement of the testpoint being instrumented.
ciscoEnvMonTemperatureStatusValue	The current temperature measurement of the testpoint being instrumented.

Operational Information:

- ciscoEnvMonShutdownNotification - Indicates an environment failure. Successive notifications can indicate the failing component. You can check the logs to collect additional information about the failure.
- ciscoEnvMonTemperatureNotification, ciscoEnvMonTempStatusChangeNotif - Indicates problems with cooling fans within device or rise in external temperature. If temperatures continue to rise device may fail.
- ciscoEnvMonVoltageNotification, ciscoEnvMonVoltStatusChangeNotif - Indicates problems with power supply. If voltage remains out of range replacement of related components may be required.
- ciscoEnvMonFanNotification, ciscoEnvMonFanStatusChangeNotif - Indicates failure of main fan or fans for power supply. You may want to check fans for obstruction of air flow or replace the system fan tray.
- ciscoEnvMonRedundantSupplyNotification, ciscoEnvMonSuppStatusChangeNotif - Indicates that a failure has occurred in the power supply. The backup power unit will provide power to device temporarily; but the failing device will need to be replaced to provide redundancy power supply. You can also try to reduce the system power consumption.
- You may want to notify your hardware support personnel of the problem.

Diagnostic Commands:

To display system status information "show environment" command inprivileged EXEC mode.

show environment [alarm | cooling | status | temperature |voltage]

alarm	(Optional) Displays environmental alarms. • status - Displays alarm status. • thresholds - Displays alarm thresholds
cooling	(Optional) Displays fan tray status, chassis cooling capacity, ambient temperature, and per-slot cooling capacity.
status	(Optional) Displays FRU operational status with power and temperature information.
temperature	(Optional) Displays FRU temperature information.
voltage	(Optional) Displays FRU voltage information.

Go Top

SECTION 4.31

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusRcvFarEndLOF	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Far End LOF.	DS1LineStatusRcvFarEndLOF	Common
DS1LineStatusRcvFarEndLOF	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Far End LOF cleared.	DS1LineStatusRcvFarEndLOF	Common
DS1LineStatusRcvFarEndLOF	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Far End LOF.	DS1LineStatusRcvFarEndLOF	Common
DS1LineStatusRcvFarEndLOF	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Far End LOF cleared.	DS1LineStatusRcvFarEndLOF	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped

	256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.32

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusXmtFarEndLOF	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Near End Sending LOF.	DS1LineStatusXmtFarEndLOF	Common
DS1LineStatusXmtFarEndLOF	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Near End Sending LOF cleared.	DS1LineStatusXmtFarEndLOF	Common
DS1LineStatusXmtFarEndLOF	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Sending LOF.	DS1LineStatusXmtFarEndLOF	Common
DS1LineStatusXmtFarEndLOF	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Sending LOF cleared.	DS1LineStatusXmtFarEndLOF	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs.

	Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.33

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusRcvAIS	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Far End Sending AIS.	DS1LineStatusRcvAIS	Common
DS1LineStatusRcvAIS	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Far End Sending AIS cleared.	DS1LineStatusRcvAIS	Common
DS1LineStatusRcvAIS	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Far End Sending AIS.	DS1LineStatusRcvAIS	Common
DS1LineStatusRcvAIS	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Far End Sending AIS cleared.	DS1LineStatusRcvAIS	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication

	8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.34

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusXmtAIS	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Near End Sending AIS.	DS1LineStatusXmtAIS	Common
DS1LineStatusXmtAIS	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Near End Sending AIS cleared.	DS1LineStatusXmtAIS	Common
DS1LineStatusXmtAIS	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Sending AIS.	DS1LineStatusXmtAIS	Common
DS1LineStatusXmtAIS	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Sending AIS cleared.	DS1LineStatusXmtAIS	Common

Description:

```
A dsx1LineStatusChange trap is sent when the               value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the

	time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.35

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusLOF	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Near End LOF.	DS1LineStatusLOF	Common
DS1LineStatusLOF	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Near End LOF cleared.	DS1LineStatusLOF	Common
DS1LineStatusLOF	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End LOF.	DS1LineStatusLOF	Common
DS1LineStatusLOF	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End LOF cleared.	DS1LineStatusLOF	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object.

	The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.36

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusLOS	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Near End LOS.	DS1LineStatusLOS	Common
DS1LineStatusLOS	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Near End LOS cleared.	DS1LineStatusLOS	Common

DS1LineStatusLOS	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End LOS.	DS1LineStatusLOS	Common
DS1LineStatusLOS	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End LOS cleared.	DS1LineStatusLOS	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service

	32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.37

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusLoopback	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Near End Is Looped.	DS1LineStatusLoopback	Common
DS1LineStatusLoopback	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Near End is Looped cleared.	DS1LineStatusLoopback	Common
DS1LineStatusLoopback	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Is Looped.	DS1LineStatusLoopback	Common
DS1LineStatusLoopback	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End is Looped cleared.	DS1LineStatusLoopback	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a

	sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusT16AIS	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to TS16 AIS.	DS1LineStatusT16AIS	Common
DS1LineStatusT16AIS	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to TS16 AIS cleared.	DS1LineStatusT16AIS	Common
DS1LineStatusT16AIS	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to TS16 AIS.	DS1LineStatusT16AIS	Common
DS1LineStatusT16AIS	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to TS16 AIS cleared.	DS1LineStatusT16AIS	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code

	4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.39

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusRcvFarEndLOMF	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Far End Sending TS16 LOMF.	DS1LineStatusRcvFarEndLOMF	Common
DS1LineStatusRcvFarEndLOMF	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Far End Sending TS16 LOMF cleared.	DS1LineStatusRcvFarEndLOMF	Common
DS1LineStatusRcvFarEndLOMF	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Far End Sending TS16 LOMF.	DS1LineStatusRcvFarEndLOMF	Common
DS1LineStatusRcvFarEndLOMF	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Far End Sending TS16 LOMF cleared.	DS1LineStatusRcvFarEndLOMF	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside

	interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.40

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusXmtFarEndLOMF	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Near End Sending TS16 LOMF.	DS1LineStatusXmtFarEndLOMF	Common
DS1LineStatusXmtFarEndLOMF	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Near End Sending TS16 LOMF cleared.	DS1LineStatusXmtFarEndLOMF	Common
DS1LineStatusXmtFarEndLOMF	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Sending TS16 LOMF.	DS1LineStatusXmtFarEndLOMF	Common
DS1LineStatusXmtFarEndLOMF	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Sending TS16 LOMF cleared.	DS1LineStatusXmtFarEndLOMF	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm)

	64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.41

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusRcvTestCode	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Near End Detects Test Code.	DS1LineStatusRcvTestCode	Common
DS1LineStatusRcvTestCode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Near End Detects Test Code cleared.	DS1LineStatusRcvTestCode	Common
DS1LineStatusRcvTestCode	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Detects Test Code.	DS1LineStatusRcvTestCode	Common
DS1LineStatusRcvTestCode	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Detects Test Code cleared.	DS1LineStatusRcvTestCode	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
```

```
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.

dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.42

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusOtherFailure	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to an Undefined Status.	DS1LineStatusOtherFailure	Common
DS1LineStatusOtherFailure	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to an Undefined Status cleared.	DS1LineStatusOtherFailure	Common
DS1LineStatusOtherFailure	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to an Undefined Status.	DS1LineStatusOtherFailure	Common
DS1LineStatusOtherFailure	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to an Undefined Status cleared.	DS1LineStatusOtherFailure	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object.

	The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.43

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusUnavailSigState	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Near End Unavailable Signal State.	DS1LineStatusUnavailSigState	Common
DS1LineStatusUnavailSigState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Near End Unavailable Signal State cleared.	DS1LineStatusUnavailSigState	Common

DS1LineStatusUnavailSigState	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Unavailable Signal State.	DS1LineStatusUnavailSigState	Common
DS1LineStatusUnavailSigState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Near End Unavailable Signal State cleared.	DS1LineStatusUnavailSigState	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service

	32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.44

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusNetEquipOOS	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to Carrier Equipment Out of Service.	DS1LineStatusNetEquipOOS	Common
DS1LineStatusNetEquipOOS	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Carrier Equipment Out of Service cleared.	DS1LineStatusNetEquipOOS	Common
DS1LineStatusNetEquipOOS	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Carrier Equipment Out of Service.	DS1LineStatusNetEquipOOS	Common
DS1LineStatusNetEquipOOS	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Carrier Equipment Out of Service cleared.	DS1LineStatusNetEquipOOS	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure,

	received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusRcvPayloadAIS	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to DS2 Payload AIS.	DS1LineStatusRcvPayloadAIS	Common
DS1LineStatusRcvPayloadAIS	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to DS2 Payload AIS cleared.	DS1LineStatusRcvPayloadAIS	Common
DS1LineStatusRcvPayloadAIS	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to DS2 Payload AIS.	DS1LineStatusRcvPayloadAIS	Common
DS1LineStatusRcvPayloadAIS	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to DS2 Payload AIS cleared.	DS1LineStatusRcvPayloadAIS	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF

	1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.46

Trap: dsx1LineStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DS1LineStatusPerfThreshold	Trap	Alarm	Yes	Major	$NodeDisplayName -- Interface $IfName line status changed to DS2 Performance Threshold Exceeded.	DS1LineStatusPerfThreshold	Common
DS1LineStatusPerfThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Interface $IfName line status changed to Performance Threshold cleared.	DS1LineStatusPerfThreshold	Common
DS1LineStatusPerfThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to DS2 Performance Threshold Exceeded.	DS1LineStatusPerfThreshold	Common
DS1LineStatusPerfThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Interface $RtrInterfaceDisplayName line status changed to Performance Threshold cleared.	DS1LineStatusPerfThreshold	Common

Description:

```
A dsx1LineStatusChange trap is sent when the                value of an instance dsx1LineStatus changes. It
can be utilized by an NMS to trigger polls.  When
the line status change results from a higher level
line status change (i.e. ds3), then no traps for
the ds1 are sent.
```

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
dsx1LineStatus	This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded
dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineIndex	This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of ifStackTable and ds0/ds0bundle mibs. Previously, this object is the identifier of a DS1 Interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same

	value as ifIndex. Otherwise, number the dsx1LineIndices with an unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g, network side) with odd numbers.

Go Top

SECTION 4.47

Status: NodeTimeZoneChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NodeTimeZoneChange	Poll	Alarm	No	Informational	Network element $NodeDisplayName shifted from TimeZone $OldNodeTimeZone to $NewNodeTimeZone.	NodeTimeZoneChange	Common

Description:

The NodeTimeZoneChange event provides information when a Node object's timezone has been shifted.

Default Message:

Network element $NodeDisplayName shifted from TimeZone $OldNodeTimeZone to $NewNodeTimeZone.

Message Substitution Variables:

NodeDisplayName

Substitution variables for Node name.	
OldNodeTimeZone	Displays the old timezone of the Node
NewNodeTimeZone	Displays the present timezone of the Node

Go Top

---

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 4.48

Status: NodeUnreachable

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NodeUnreachable	Poll	Alarm	Yes	Critical	Node $NodeDisplayName is unreachable.	NodeUnreachable	Common
NodeUnreachable	Poll	Alarm	Yes	Normal	Node $NodeDisplayName is reachable.	NodeUnreachable	Common

Description:

The NodeUnreachable event indicates that MWTM can not query a device via SNMP. This event may occur when MWTM does not have the correct SNMP community string for the device or when the the device becomes otherwise unresponsive.

Default Message:

- Node $NodeDisplayName is unreachable.
- Node $NodeDisplayName is reachable.

Message Substitution Variables:

state
reason of the Node.

Node	Substitution variables for Node related data.
NodeState	The current state of the Node.
NodeStateReason	
NodeLastState	The previous state of the Node.
NodeReachableState	The reachability state of this node. Reachable or Unreachable

Operational Information:

- Check that the SNMP community string provided to MWTM for this device is correct.
- Ping and telnet to the device to further investigate the device status.

Go Top

SECTION 4.49

Status: TrapRateStatus-Onset,TrapRateStatus-Minor and TrapRateStatus-Abate

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
TrapRateStatus	Poll	Alarm	Yes	Critical	Node $NodeDisplayName is generating too many traps. MWTM has stopped trap processing for this node. MWTM will re-enable trap processing in approximately $RescueTime minutes.	TrapRateStatus	Common
TrapRateStatus	Poll	Alarm	Yes	Minor	Node $NodeDisplayName trap rate exceeds threshold level of $MinorThreshold.	TrapRateStatus	Common
TrapRateStatus	Poll	Alarm	Yes	Normal	Node $NodeDisplayName $Message	TrapRateStatus	Common

Description:

The TrapRateStatus - Minor alarm indicates that the node has started generating too many traps within a short duration and the count has exceeded the minor threshold limit. The alarm will automatically be cleared if the trap count comes below the abate threshold within the configurable time duration. This is a 'Minor' status trap.

The TrapRateStatus - Onset alarm indicates that the node is generating too many traps within a short duration. MWTM detects this trap storm condition and stops further trap processing of the node. The node's 'ProcessTrap' flag is set to False. MWTM will automatically re-enable trap processing for this node within a configurable time duration.
This is a 'Critical' status trap.

The TrapRateStatus - Abate alarm indicates that MWTM has re-enabled trap processing for this node. The node's 'ProcessTrap' flag is set to True. This is a 'Normal' status trap.

Default Message:

Node $NodeDisplayName is generating too many traps. MWTM has stopped trap processing for this node. MWTM will re-enable trap processing in approximately $RescueTime minutes.

Node $NodeDisplayName is automatically re-enabled for trap processing by MWTM.

Node $NodeDisplayName trap rate exceeds threshold level of $MinorThreshold.

Node $NodeDisplayName trap rate returned to normal.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
RescueTime	Indicates an approximate time after which MWTM automatically re-enables trap processing.
MinorThreshold	Indicates the count above which the minor alarm will be triggered.

Operational Information:

- Analyze the traps generated for this node. The trap information can indicate the problem found on the device.
- To view the nodes which are currently have the Process Traps set to 'No', select 'Nodes' option in the Summary Lists and sort on the Process Trap column. It can also be viewed on the 'Details' tab for each node.

Go Top

SECTION 4.50

Status: RebootDetected

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FailoverDetected	Poll	Alarm	No	Warning	Router failover/hardware replacement detected for $NodeDisplayName. Last known sysUpTime is $SysUpTime.	FailoverDetected	Common

Description:

The RebootDetected status event provides information when MWTM detects that a reboot has occurred on a Node.

Default Message:

Router reboot detected for $NodeDisplayName. Last known sysUpTime is $SysUpTime.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
SysUpTime	The amount of time the router has been active since the reboot.

Operational Information:

Some problem has occurred on the device to cause a reboot. It can also be a software reboot on the device. In which case the configuration might have been modified.
You may want to investigate with your IP administrator why the router was rebooted.

Go Top

SECTION 4.51

Status: SnmpError

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SnmpError	Poll	Alarm	No	Warning	Node $NodeDisplayName is not a supported device or does not have the minimum IOS mib level.	SnmpError	Common
SnmpError	Poll	Alarm	No	Minor	Node $NodeDisplayName encountered an error during polling: $ErrorString.	SnmpError	Common
SnmpError	Poll	Alarm	No	Warning	Node $NodeDisplayName has not been configured.	SnmpError	Common

Description:

The SnmpError status event provides information when MWTM experiences an error during a poll of a Node. The value of SnmpErrorType indicates the type of error. Possible values of SnmpErrorType include:

- NotSnmpable - The Node has no SNMPable interfaces.
- UnsupportedDevice - The Node is not a supported device.
- MibError - An unexpected error occurred.
- NotConfigured - The Node is not configured as an RAN-O device.

Default Message:

- Node $NodeDisplayName has no snmp-able addresses to poll.
- Node $NodeDisplayName is not a supported device or does not have the minimum IOS mib level.
- Node $NodeDisplayName encountered and error during polling: $ErrorString.
- Node $NodeDisplayName has not been configured for a particular MWTM personality.

Message Substitution Variables:

Node

Substitution variables for Node related data.	

SnmpErrorType	Indicates the type of error that occurred.
ErrorString	A detailed error message relative only when ErrorType is MibError.

Operational Information:

- When SnmpErrorType is NotSnmpable check that the Node has not been configured in MWTM to have no SNMPable interfaces. This is most likely a user error.
- When SnmpErrorType is UnsupportedDevice the node is not a supported device or does not have the minimum IOS mib level required by MWTM.
- When SnmpErrorType is MibError an unexpected error has occurred polling a Node. The MessageLog.txt file may have more information related to the error. An ErrorString of 'NoSuchInstance' can occur if MWTM is using a read community string of 'public' for a router but the router has been configured with a non 'public' read community string.
- When SnmpErrorType is NotConfigured the Node is a valid router however it has not been configured for a particular MWTM personality.
- This status could also indicate that device is being accessed via a wrong community string. You can use the MWTM Node SNMP and Credentials Editor to check community strings.

Go Top

SECTION 4.52

Status: DeviceConfigDownload

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ConfigurationDownload	Poll	Alarm	Yes	Minor	$NodeDisplayName -- Device configuration download Failed. Reason: FailedReason	ConfigurationDownload	Common
ConfigurationDownload	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Device configuration download Succeeded.	ConfigurationDownload	Common

Description:

The DeviceConfigDownload status event provides information when MWTMperforms a device configuration download task.

Default Message:

- $NodeDisplayName -- Device configuration download $ConfigDownloadStatus. Reason: $ConfigDownloadStatusReason

Message Substitution Variables:

Node	Substitution variables for Node related data.
ConfigDownloadStatus	Possible values are Succeeded or Failed.
ConfigDownloadStatusReason	This value is empty if the task succeeded, otherwise, a failure reason.

Operational Information:

- If the download status is 'Succeeded' no action is required.
- If the download status is 'Failed' it indicates that MWTM is unable to access the node. The ITP could be facing some network connectivity issues. It can indicate that the device is being accessed via the wrong protocol (SSH or telnet) or via the wrong SNMP community string. You may want to check this information using the MWTM Node SNMP and Credentials Editor.

Go Top

---

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 4.53

Status: MemoryBufferElementsFree

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MemoryBufferElementsFree	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The memory buffer elements free threshold is Acceptable. Value $MemoryBufferElementsFreeValue	MemoryBufferElementsFree	Common
MemoryBufferElementsFree	Poll	Alarm	Yes	Major	$NodeDisplayName -- The memory buffer elements free threshold is Exceeded. Value	MemoryBufferElementsFree	Common

					$MemoryBufferElementsFreeValue		

Description:

The number of free buffer elements.

Default Message:

$NodeDisplayName -- The memory buffer elements free threshold is
$MemoryBufferElementsFreeState. Value
$MemoryBufferElementsFreeValue

Message Substitution Variables:

Node	Substitution variables for Node related data.
MemoryBufferElementsFreeState	Acceptable or Exceeded
MemoryBufferElementsFreeValue	The bufferElFree value

Go Top

---

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 4.54

Status: FreeMemory

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FreeMemory	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The free memory threshold is Acceptable. Value $FreeMemoryValue	FreeMemory	Common
FreeMemory	Poll	Alarm	Yes	Major	$NodeDisplayName -- The free memory threshold is Exceeded. Value $FreeMemoryValue	FreeMemory	Common

Description:

Chassis free memory value.

Default Message:

$NodeDisplayName -- The free memory threshold is $FreeMemoryState.
Value $FreeMemoryValue

Message Substitution Variables:

Node	Substitution variables for Node related data.
FreeMemoryState	Acceptable or exceeded
FreeMemoryValue	The value of freeMem

Go Top

---

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 4.55

Status: ChassisPowerSupply1

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChassisPowerSupply1	Poll	Alarm	Yes	Minor	$NodeDisplayName -- The chassis power supply 1 has a fault.	ChassisPowerSupply1	Common
ChassisPowerSupply1	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The chassis power supply 1 is normal.	ChassisPowerSupply1	Common

Description:

The status of power supply 1.

Default Message:

$NodeDisplayName -- The chassis power supply 1 has a fault.

Message Substitution Variables:

Node	Substitution variables for Node related data.
ChassisPowerSupply1State	Normal or Fault

Go Top

---

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 4.56

Status: ChassisPowerSupply2

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChassisPowerSupply2	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The chassis power supply 2 is normal.	ChassisPowerSupply2	Common
ChassisPowerSupply2	Poll	Alarm	Yes	Minor	$NodeDisplayName -- The chassis power supply 2 has a fault.	ChassisPowerSupply2	Common

Description:

The status of power supply 1.

Default Message:

$NodeDisplayName -- The chassis power supply 2 has a fault.

Message Substitution Variables:

Node	Substitution variables for Node related data.
ChassisPowerSupply2State	Normal or Fault

Go Top

---

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 4.57

Status: CpmCPUavgBusy5

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CpmCPUavgBusy5	Poll	Alarm	Yes	Normal	$NodeDisplayName - The CPU 5 minute average utilization value($cpmCPUavgBusy5Value) for $entPhyDes has Acceptable threshold.	CpmCPUavgBusy5	Common
CpmCPUavgBusy5	Poll	Alarm	Yes	Warning	$NodeDisplayName - The CPU 5 minute average utilization value($cpmCPUavgBusy5Value) for $entPhyDes has Exceeded threshold.	CpmCPUavgBusy5	Common

Description:

The 5 minute exponentially decaying moving average of the CPU busy percentage.

Default Message:

$NodeDisplayName - The CPU 5 minute average utilization value($cpmCPUavgBusy5Value) for $entPhyDes has $cpmCPUavgBusy5State threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data.
cpmCPUavgBusy5State	Acceptable or Exceeded
cpmCPUavgBusy5Value	The CPU 5 minute average utilization value
entPhyDes	CPU description

Go Top

Status: ChassisTempAlarmState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChassisTempAlarm	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Chassis temperature alarm cleared.	ChassisTempAlarm	Common
ChassisTempAlarm	Poll	Alarm	Yes	Major	$NodeDisplayName -- Chassis temperature alarm reported.	ChassisTempAlarm	Common
ChassisTempAlarm	Poll	Alarm	Yes	Critical	$NodeDisplayName -- Chassis temperature is critical.	ChassisTempAlarm	Common

Description:

This status alarm is generated when the mib variable 'chassisMajorAlarm' transitions between the 'off', and 'on' states.

Default Messages:

- $NodeDisplayName -- Chassis temperature is critical.
- $NodeDisplayName -- Chassis temperature alarm reported.
- $NodeDisplayName -- Chassis temperature is normal.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
chassisTempAlarm	The chassis temperature alarm status. The states are: off -- temperature within normal range on -- temperature too high critical -- critical temperature, system shut down imminent

Operational Information:

- If the chassis temperature is too high, a minor or major alarm can be generated. You can inspect the indicated component closely to determine why it is operating out of the normal operating temperature range and whether it will eventually exceed the allowed operating temperature range.
- This alarm can indicate a redundant power supply has been powered off. You may want to replace the FRU.
- This alarm can also indicate that one or more fans in the system fan tray have failed. You can replace the system fan tray to fix the problem.

Diagnostic Commands:

To display system status information "show environment" command in privileged EXEC mode.

show environment [alarm | cooling | status | temperature | voltage]

alarm	(Optional) Displays environmental alarms. • status - Displays alarm status. • thresholds - Displays alarm thresholds
	(Optional) Displays fan tray status, chassis cooling capacity,

cooling	ambient temperature, and per-slot cooling capacity.
status	(Optional) Displays FRU operational status with power and temperature information.
temperature	(Optional) Displays FRU temperature information.
voltage	(Optional) Displays FRU voltage information.

Go Top

Status: ChassisMajorAlarmState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChassisMajorAlarm	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Chassis major alarm cleared.	ChassisMajorAlarm	Common
ChassisMajorAlarm	Poll	Alarm	Yes	Major	$NodeDisplayName -- Chassis has a major alarm.	ChassisMajorAlarm	Common

Description:

This status alarm is generated when the mib variable 'chassisMajorAlarm' transitions between the 'off', and 'on' states.

Default Messages:

- $NodeDisplayName -- Chassis does not have a major alarm.
- $NodeDisplayName -- Chassis has a major alarm.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
chassisMajorAlarm	The chassis major alarm status. The states are 'off' and 'on'.

Operational Information:

- If the chassis temperature is too high, a minor or major alarm can be generated. You can inspect the indicated component closely to determine why it is operating out of the normal operating temperature range and whether it will eventually exceed the allowed operating temperature range.
- This alarm can indicate a redundant power supply has been powered off. You may want to replace the FRU.
- This alarm can also indicate that one or more fans in the system fan tray have failed. You can replace the system fan tray to fix the problem.

Diagnostic Commands:

To display system status information "show environment" command in privileged EXEC mode.

show environment [alarm | cooling | status | temperature | voltage]

alarm	(Optional) Displays environmental alarms. • status - Displays alarm status. • thresholds - Displays alarm thresholds
cooling	(Optional) Displays fan tray status, chassis cooling capacity, ambient temperature, and per-slot cooling capacity.
status	(Optional) Displays FRU operational status with power and temperature information.
temperature	(Optional) Displays FRU temperature information.
voltage	(Optional) Displays FRU voltage information.

Go Top

Status: ChassisMinorAlarmState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChassisMinorAlarm	Poll	Alarm	Yes	Minor	$NodeDisplayName -- Chassis has a minor alarm.	ChassisMinorAlarm	Common
ChassisMinorAlarm	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Chassis minor alarm cleared.	ChassisMinorAlarm	Common

Description:

This status alarm is generated when the mib variable 'chassisMinorAlarm' transitions between the 'off', and 'on' states.

Default Messages:

- $NodeDisplayName -- Chassis does not have a minor alarm.
- $NodeDisplayName -- Chassis has a minor alarm.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
chassisMinorAlarm	The chassis Minor alarm status. The states are 'off' and 'on'.

Operational Information:

- If the chassis temperature is too high, a minor or major alarm can be generated. You can inspect the indicated component closely to determine why it is operating out of the normal operating temperature range and whether it will eventually exceed the allowed operating temperature range.
- This alarm can indicate a redundant power supply has been powered off. You may want to replace the FRU.
- This alarm can also indicate that one or more fans in the system fan tray have failed. You can replace the system fan tray to fix the problem.

Diagnostic Commands:

To display system status information "show environment" command in privileged EXEC mode.

show environment [alarm | cooling | status | temperature | voltage]

alarm	(Optional) Displays environmental alarms. • status - Displays alarm status. • thresholds - Displays alarm thresholds
cooling	(Optional) Displays fan tray status, chassis cooling capacity, ambient temperature, and per-slot cooling capacity.
status	(Optional) Displays FRU operational status with power and temperature information.
temperature	(Optional) Displays FRU temperature information.
voltage	(Optional) Displays FRU voltage information.

Go Top

Status: MWTMDatabaseError

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MWTMDatabaseError	Poll	Alarm	No	Critical	MWTM Database integrity check detected an error. $ErrorString	MWTMDatabaseError	Common

Description:

The MWTMDatabaseError status event provides information when MWTM experiences an unexpected error during the nightly database integrity check. The value of MWTMDatabaseErrorType indicates the type of error. Possible values of MWTMDatabaseErrorType include:

- ErrorDetected

Default Message:

MWTM Database integrity check detected an error. $ErrorString

Message Substitution Variables:

MWTMDatabaseErrorType	Indicates the type of error that occurred. Currently, only ErrorDetected is supported.
ErrorString	A detailed error message describing the error.

Operational Information:

- By default this event will raise a critical alarm. It indicates that some type of error occurred during the nightly database integrity check.
- The exact error will be indicated by $ErrorString.
- Please contact MWTM support personnel along with 'mwtm tac' output as soon as possible.

Go Top

SECTION 4.62

Status: MWTMDiskUtilization

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MWTMDiskUtilization	Poll	Alarm	No	Critical	MWTM Server has exceeded the minimum disk space requirement of $MinRequired for partition: $Partition. Space left = $FreeSpace.	MWTMDiskUtilization	Common
MWTMDiskUtilization	Poll	Alarm	No	Major	MWTM Server is approaching the minimum disk space requirement of $MinRequired for partition: $Partition. Space left = $FreeSpace.	MWTMDiskUtilization	Common

Description:

The MWTMDiskUtilization status event is created when the MWTM server disk utilization is approaching or exceeding the minimum free space required for continued operation.

Default Message:

- MWTM Server has exceeded the minimum disk space requirement of $MinRequired for partition: $Partition. Space left = $FreeSpace.
- MWTM Server is approaching the minimum disk space requirement of $MinRequired for partition: $Partition. Space left = $FreeSpace.

Message Substitution Variables:

MinRequired	The mimimum free space required for continued operation
Partition	The disk partition on which the disk utilization measurement is taken
FreeSpace	The amount of free space left on the disk partition

Operational Information:

- Review the contents of the disk partition named in this event and attempt to free up additional space.

Go Top

SECTION 4.63

Status : MWTMCriticalAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MWTMCriticalAlarm	Poll	Alarm	No	Critical	Critical Alarm: $MessageText	MWTMCriticalAlarm	Common

Go Top

SECTION 4.64

Status : MWTMMajorAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MWTMMajorAlarm	Poll	Alarm	No	Major	Major Alarm: $MessageText	MWTMMajorAlarm	Common

Go Top

SECTION 4.65

Status : MWTMMinorAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MWTMMinorAlarm	Poll	Alarm	No	Minor	Minor Alarm: $MessageText	MWTMMinorAlarm	Common

Go Top

SECTION 4.66

Status : MWTMWarningAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MWTMWarningAlarm	Poll	Alarm	No	Warning	Warning Alarm: $MessageText	MWTMWarningAlarm	Common

Go Top

SECTION 4.67

Status : MWTMInformationalAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MWTMInformationalAlarm	Poll	Alarm	No	Informational	Informational Alarm: $MessageText	MWTMInformationalAlarm	Common

Go Top

SECTION 4.68

Status : MWTMNormalAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MWTMNormalAlarm	Poll	Alarm	No	Normal	Normal Alarm: $MessageText	MWTMNormalAlarm	Common

Go Top

Status: RedundancyState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RedundancyState	Poll	Alarm	No	Major	$NodeDisplayName -- The redundancy state changed to active.	RedundancyState	Common
RedundancyState	Poll	Alarm	No	Major	$NodeDisplayName -- The redundancy state changed to standby hot.	RedundancyState	Common
RedundancyState	Poll	Alarm	No	Major	$NodeDisplayName -- The redundancy state changed to $cRFStatusUnitState.	RedundancyState	Common

Description:

This event is created when a redundancy state change occurs as indicated by the cRFStatusUnitState mib object.

Default Message:

$NodeDisplayName -- The redundancy state changed to active.
$NodeDisplayName -- The redundancy state changed to standby hot.
$NodeDisplayName -- The redundancy state changed to $cRFStatusUnitState.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
cRFStatusUnitState	notKnown - state is unknown disabled - RF is not operational on this unit initialization - establish necessary system services negotiation - peer unit discovery and negotiation standbyCold - client notification on standby unit *standbyColdConfig - standby cfg is updated from active cfg *standbyColdFileSys - standby file system (FS) is updated from the active FS *standbyColdBulk - clients sync data from active to standby standbyHot - incremental client data sync continues. This unit is ready to take over activity. activeFast - call maintenance efforts during a SWACT activeDrain - client clean-up phase activePreconfig - unit is active but has not read its configuration activePostconfig - unit is active and is post-processing its configuration active - unit is active and processing calls activeExtraload - unit is active and processing calls for all feature boards in the system activeHandback - unit is active, processing calls and is in the process of handing some resources to the other unit in the system * Sub-state of 'standbyCold'

Operational Information:

- You may want to use the crashfile or the bootflash device to determine the cause for state change. You can also check the logs to determine if state change was at operators request.
- Based on the redundancy mode there may be some link failure and the system may not be able to carry traffic.

Diagnostic Commands:

To monitor CPU switch module redundancy operations, use the following show command.

show redundancy [clients | counters | events | history | idb-sync-history | linecard-groupstates | states | switchover]

clients	(Optional) Displays list of internal redundancy clients.
counters	(Optional) Displays internal redundancy software counters.
events	(Optional) Displays internal redundancy events.
history	(Optional) Displays internal redundancy software history.
idb-sync-history	(Optional) Displays internal redundancy IDB sync history.
linecard-groupstates	(Optional) Displays line card redundancy group information.
states	(Optional) Displays internal redundancy software states.
switchover	(Optional) Displays internal redundancy switchover.

Go Top

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 4.70

Status: SystemFreeMemory

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SystemFreeMemory	Poll	Alarm	Yes	Normal	The System free memory threshold for the system is Acceptable. Value $SystemFreeMemoryValue	SystemFreeMemory	Common
SystemFreeMemory	Poll	Alarm	Yes	Warning	The System free memory threshold for the system is Warning. Value $SystemFreeMemoryValue	SystemFreeMemory	Common
SystemFreeMemory	Poll	Alarm	Yes	Critical	The System free memory threshold for the system is Critical. Value $SystemFreeMemoryValue	SystemFreeMemory	Common

Description:

System free memory value.

Default Message:

The System free memory threshold is $SystemFreeMemoryState.
Value $SystemFreeMemoryValue

Message Substitution Variables:

SystemFreeMemoryState	Acceptable or Warning or Critical
SystemFreeMemoryValue	The value of system free memory

Go Top

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 4.71

Status: EnhancedFreeMemoryPoolState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EnhancedFreeMemoryState	Poll	Alarm	Yes	Warning	$NodeDisplayName -- Memory Utilization of $EnhancedFreeMemoryPoolDescr $EnhancedFreeMemoryPoolName of type $EnhancedFreeMemoryPoolType is Exceeded with Free memory value $EnhancedFreeMemoryPoolValue Bytes	EnhancedFreeMemoryState	Common
EnhancedFreeMemoryState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Memory Utilization of $EnhancedFreeMemoryPoolDescr $EnhancedFreeMemoryPoolName of type $EnhancedFreeMemoryPoolType is Acceptable with Free memory value $EnhancedFreeMemoryPoolValue Bytes	EnhancedFreeMemoryState	Common

Description:

Free memory value from of CISCO-ENHANCED-MEMORY-POOL mib.

Default Message:

$NodeDisplayName -- Memory Utilization of $EnhancedFreeMemoryPoolDescr $EnhancedFreeMemoryPoolName of type $EnhancedFreeMemoryPoolType is $EnhancedFreeMemoryPoolState with Free memory value $EnhancedFreeMemoryPoolValue Bytes

Message Substitution Variables:

Node	Substitution variables for Node related data.
EnhancedFreeMemoryPoolState	Acceptable or exceeded
EnhancedFreeMemoryPoolValue	The value of
EnhancedFreeMemoryPoolName	The memory pool name
EnhancedFreeMemoryPoolDescr	The memory pool description

EnhancedFreeMemoryPoolType	The memory pool type

Go Top

content="Mozilla/4.73 [en]C-CCK-MCD (WinNT; U) [Netscape]">SECTION 4.72

Status: FreeMemoryPoolState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FreeMemoryState	Poll	Alarm	Yes	Warning	$NodeDisplayName -- Memory Utilization of $FreeMemoryPoolName is Exceeded Free memory with value $FreeMemoryPoolValue Bytes	FreeMemoryState	Common
FreeMemoryState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- Memory Utilization of $FreeMemoryPoolName is Acceptable with Free memory value $FreeMemoryPoolValue Bytes	FreeMemoryState	Common

Description:

Free memory value from ciscoMemoryPoolFree of CISCO-MEMORY-POOL mib.

Default Message:

"$NodeDisplayName -- Memory Utilization of $FreeMemoryPoolName is $FreeMemoryPoolState Free memory with value $FreeMemoryPoolValue Bytes".

Message Substitution Variables:

Node	Substitution variables for Node related data.
FreeMemoryPoolState	Acceptable or exceeded
FreeMemoryPoolValue	The value of ciscoMemoryPoolFree
FreeMemoryPoolName	The memory pool name

Go Top

SECTION 4.73

Trap : UnknownTrap

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
UnknownTrap	Trap	Event	No	Informational	A trap ($TrapName) was received for node $HostAddress	UnknownTrap	Common

Go Top

SECTION 4.74

Trap: ciscoRFSwactNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NsoActive	Trap	Event	No	Warning	$NodeDisplayName - Redundant unit $UnitId now active. Switch reason: $RFSwitchReason.	NsoActive	Common

Description:

This trap is sent by a newly active redundant unit whenever a switch of activity occurs. In the case where a switch event may be indistinguishable from a reset event, a network management station should use this trap to differentiate the activity.

Switch of Activity (SWACT) indicates either a forced or automatic switch of active status from the active unit to the standby unit. The former standby unit is now referred to as the active unit.

The value of RFSwitchReason indicates the reason for the switch. Possible values of RFSwitchReason include:

- Unsupported - the 'reason code' is an unsupported feature.
- None - no switch has occurred.
- NotKnown - reason is unknown.
- UserInitiated - a safe, manual switch was initiated by an administrator.
- UserForced - a manual switch was forced by an administrator; ignoring pre-conditions, warnings and safety checks.
- ActiveUnitFailed - active unit failure caused an auto switch.
- ActiveUnitRemoved - active unit removal caused an auto switch.

Default Message:

$NodeDisplayName ($NodeCliCode) - Redundant unit $UnitId now active. Switch reason: $RFSwitchReason.

Message Substitution Variables:

CommonNode

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.	
RFSwitchReason	The reason for the last switch of activity.
UnitId	A unique identifier for this redundant unit. This identifier is implementation-specific but the method for selecting the id must remain consistent throughout the redundant system. Some example identifiers include: slot id, physical or logical entity id, or a unique id assigned internally by the RF subsystem.

Operational Information:

- If the switch reason is 'UserInitiated', 'UserForced', or 'ActiveUnitRemoved' contact the administrator responsible for the switch.
- If the switch reason is any other reason there is a hardware or software problem that needs to be addressed.
- You may want to use the crashfile or the bootflash device to determine the cause for state change. You can also check the logs to determine if state change was at operators request.
- Based on the redundancy mode there may be some link failure and the system may not be able to carry traffic.

Diagnostic Commands:

To monitor CPU switch module redundancy operations, use the following show command.

show redundancy [clients | counters | events | history | idb-sync-history | linecard-groupstates | states | switchover]

clients	(Optional) Displays list of internal redundancy clients.
counters	(Optional) Displays internal redundancy software counters.
events	(Optional) Displays internal redundancy events.
history	(Optional) Displays internal redundancy software history.
idb-sync-history	(Optional) Displays internal redundancy IDB sync history.
linecard-groupstates	(Optional) Displays line card redundancy group information.
states	(Optional) Displays internal redundancy software states.
switchover	(Optional) Displays internal redundancy switchover.

Go Top

SECTION 4.75

Trap: ciscoRFProgressionNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NsoState	Trap	Event	No	Major	$NodeDisplayName - Redundancy states changed. Active Unit ID/State: $ActiveUnitId/$ActiveUnitState Peer Unit ID/State: $PeerUnitId/$PeerUnitState .	NsoState	Common

Description:

This trap is sent by the active redundant unit whenever its RF state changes or the RF state of the peer unit changes. To avoid a flurry of notifications for all state transitions,

notifications will only be sent for transitions to the following RF states: standbyCold, standbyHot, active, and activeExtraload.

Progression indicates the process of making redundancy state of the standby unit equivalent to that of the active unit. This includes transitioning the RF state machine through several states which drives the RF clients on the active unit to synchronize any relevant data with their peer on the standby unit.

Default Message:

$NodeDisplayName ($NodeCliCode) - Redundancy states changed. Active Unit ID/State: $ActiveUnitId/$ActiveUnitState Peer Unit ID/State: $PeerUnitId/$PeerUnitState.

Message Substitution Variables:

CommonNode

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.	
ActiveUnitId	A unique identifier for this redundant unit. This identifier is implementation-specific but the method for selecting the id must remain consistent throughout the redundant system. Some example identifiers include: slot id, physical or logical entity id, or a unique id assigned internally by the RF subsystem.
ActiveUnitState	The current state of RF on this unit.
PeerUnitId	A unique identifier for this redundant unit. This identifier is implementation-specific but the method for selecting the id must remain consistent throughout the redundant system. Some example identifiers include: slot id, physical or logical entity id, or a unique id assigned internally by the RF subsystem.
PeerUnitState	The current state of RF on this unit.

Operational Information:

- The existence of this trap indicates the state of the redundancy feature of the router is in flux and should be investigated by the router administrator.
- You may want to use the crashfile or the bootflash device to determine the cause for state change. You can also check the logs to determine if state change was at operators request.

Diagnostic Commands:

To monitor CPU switch module redundancy operations, use the following show command.

show redundancy [clients | counters | events | history | idb-sync-history | linecard-groupstates | states | switchover]

clients	(Optional) Displays list of internal redundancy clients.
counters	(Optional) Displays internal redundancy software counters.
events	(Optional) Displays internal redundancy events.
history	(Optional) Displays internal redundancy software history.
idb-sync-history	(Optional) Displays internal redundancy IDB sync history.
linecard-groupstates	(Optional) Displays line card redundancy group information.
states	(Optional) Displays internal redundancy software states.
switchover	(Optional) Displays internal redundancy switchover.

Go Top

SECTION 4.76

Trap: cpmCPURisingThreshold and cpmCPUFallingThreshold

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CPUThreshold	Trap	Event	No	Warning	$NodeDisplayName ($NodeCliCode) - $CPUThresholdClass CPU utilization $TotalCPUUtilization% is above threshold of $RisingThreshold%. Processes: (Pid/Util) $Processes	CPUThreshold	Common
CPUThreshold	Trap	Event	No	Normal	$NodeDisplayName ($NodeCliCode) - $CPUThresholdClass CPU utilization $TotalCPUUtilization% is below threshold of $FallingThreshold%.	CPUThreshold	Common

Description:

These traps notify network management applications of changes in router cpu utilization.

A cpmCPURisingThreshold notification is sent when configured rising CPU utilization threshold (cpmCPURisingThresholdValue) is reached and CPU utilization remained above the threshold for configured interval (cpmCPURisingThresholdPeriod) and such a notification is requested.
The cpmProcExtUtil5SecRev and cpmProcessTimeCreated objects can be repeated multiple times in a notification indicating the top users of CPU.

Default Message:

- $NodeDisplayName ($NodeClliCode) - $CPUThresholdClass CPU utilization $TotalCPUUtilization% is above threshold of $RisingThreshold%.
  Processes: (Pid/Util) $Processes
- $NodeDisplayName ($NodeClliCode) - $CPUThresholdClass CPU utilization $TotalCPUUtilization% is below threshold of $FallingThreshold%.

Message Substitution Variables:

CommonNode

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the SGM database based on the IP address of the ITP router that sent the trap.	
CPUThresholdClass	The type of cpu utilization. May be Interrupt, Process, or Total.
RisingThreshold	The percentage rising threshold value configured by the user. (cpmCPURisingThreshold only)
FallingThreshold	The percentage falling threshold value configured by the user. (cpmCPUFallingThreshold only)
Processes	The top cpu using processes running on the router in the format: process id / cpu utilization %. (cpmCPURisingThreshold only) 4175 characters, 594 words, 116 lines
TotalCPUUtilization	Total CPU Utilization
InterruptCPUUtilization	Interrupt CPUU tilization

Operational Information:

- If the utilization state is under threshold then no action is necessary.
- If the utilization state is over threshold then you may want to examine the CPU usage of each process running on the router to help determine the cause of the high overall cpu utilization. The increase in CPU usage can be due to processing at higher traffic levels or attacks. You can reduce traffic or perform operations like flash formatting during off peak times.

Diagnostic Commands:

1. To display information about the active processes, use the show processes command in privileged EXEC mode.

show processes [history | *pid*]

history	(Optional) Displays the process history in an ordered format.
pid	(Optional) An integer that specifies the process for which memory and CPU utilization data shall be returned.

2. To display detailed CPU utilization statistics (CPU use per process), use the show processes command in privileged EXEC mode.

show processes cpu [history | sorted]

history	(Optional) Displays CPU history in a graph format.
sorted	(Optional) Displays CPU history sorted by percentage of utilization.

3. To display amount of system memory used per system process, use the show processes memory in privileged EXEC mode.

show processes memory

Configuration Commands:

1. To configure IOS to generate CPU Threshold Traps refer to the following link in the IOS Configuration Guide.

- IOS Config Guide

Go Top

SECTION 4.77

Trap: ciscoConfigManEvent

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
HistoryEventConfigDestination	Trap	Event	No	Warning	The running configuration changed on $NodeDisplayName. Command Source: $ccmHistoryEventCommandSource, Config Source: $ccmHistoryEventConfigSource, Config Destination: running	HistoryEventConfigDestination	Common
HistoryEventConfigDestination	Trap	Event	No	Informational	A configuration management event occurred on $NodeDisplayName. Command Source: commandLine, Config Source: running, Config Destination: commandSource	HistoryEventConfigDestination	Common

Description:

Notification of a configuration management event as recorded inccmHistoryEventTable.

Default Message:

A configuration management event occurred on $NodeDisplayName. Command Source: $ccmHistoryEventCommandSource, Config Source: $ccmHistoryEventConfigSource, Config Destination: $ccmHistoryEventConfigDestination

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccmHistoryEventCommandSource	The source of the command that instigated the event. The values are: • snmp • commandLine
ccmHistoryEventConfigSource and ccmHistoryEventConfigDestination	The configuration data source / destination for the event. The values are: • erase - erasing destination (source only) • commandSource - live operational data • running - the command source itself • startup - config the system will use next reboot • local - local NVRAM or flash • networkTftp - network host via Trivial File Transfer • networkRcp - network host via Remote Copy • networkFtp - network host via File transfer • networkScp - network host via Secure Copy

Operational Information:

- This is an informational trap that indicates write mem or the some configuration change has occurred on the device.

Go Top

SECTION 4.78

Trap: ciscoConfigManEvent

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ConfigManEvent	Trap	Event	No	Informational	A configuration management event occurred on $NodeDisplayName. Command Source: $ccmHistoryEventCommandSource, Config Source: $ccmHistoryEventConfigSource, Config Destination: $ccmHistoryEventConfigDestination	ConfigManEvent	Common

Description:

Notification of a configuration management event as recorded inccmHistoryEventTable.

Default Message:

A configuration management event occurred on $NodeDisplayName. Command Source: $ccmHistoryEventCommandSource, Config Source: $ccmHistoryEventConfigSource, Config Destination: $ccmHistoryEventConfigDestination

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccmHistoryEventCommandSource	The source of the command that instigated the event. The values are: • snmp • commandLine
ccmHistoryEventConfigSource and ccmHistoryEventConfigDestination	The configuration data source / destination for the event. The values are: • erase - erasing destination (source only) • commandSource - live operational data • running - the command source itself • startup - config the system will use next reboot • local - local NVRAM or flash • networkTftp - network host via Trivial File Transfer • networkRcp - network host via Remote Copy • networkFtp - network host via File transfer • networkScp - network host via Secure Copy

Operational Information:

- This is an informational trap that indicates write mem or the some configuration change has occurred on the device.

Go Top

Trap: ccmCLIRunningConfigChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CLIRunningConfigChanged	Trap	Event	No	Informational	The running configuration on $NodeDisplayName was change via the CLI. Terminal Type: $ccmHistoryEventTerminalType	CLIRunningConfigChanged	Common

Description:

This notification indicates that the running configuration of themanaged system has changed from the CLI. If the managed system supports a separate configuration mode (where the configuration commands are

entered under a configuration session which affects the running configuration of the system), then this notification is sent when the configuration mode is exited. During this configuration session there can be one or more running configuration changes.

Default Message:

The running configuration on $NodeDisplayName was change via the CLI.
Terminal Type: $ccmHistoryEventTerminalType

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccmHistoryRunningLastChanged	The value of sysUpTime when the running configuration was last changed.
ccmHistoryEventTerminalType	If ccmHistoryEventCommandSource is 'commandLine', the terminal type, otherwise 'notApplicable'.

Operational Information:

- This is an informational trap. If the value of ccmHistoryRunningLastChanged is greater than ccmHistoryRunningLastSaved, the configuration has been changed but not saved.

Go Top

SECTION 4.80

Trap: cHsrpStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
HSRPState	Trap	Event	No	Major	The HSRP state on $NodeDisplayName changed to $cHsrpGrpStandbyState.	HSRPState	Common
HSRPState	Trap	Event	No	Major	The HSRP state on $NodeDisplayName changed to active.	HSRPState	Common
HSRPState	Trap	Event	No	Major	The HSRP state on $NodeDisplayName changed to standby.	HSRPState	Common

Description:

A cHsrpStateChange notification is sent when a cHsrpGrpStandbyStatetransitions to either active or standby state, or leaves active or standby state. There will be only one notification issued when the state change is from standby to active and vice versa.

Default Message:

The HSRP state on $NodeDisplayName changed to $cHsrpGrpStandbyState.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cHsrpGrpStandbyState	The current HSRP state of this group on this interface. initial(1), learn(2), listen(3), speak(4), standby(5), active(6)

Operational Information:

- If the state is 'Initial' then it indicates that HSRP is not running. This state is entered via a configuration change or when an interface first comes up.
- If the state is 'Learn' then it indicates that the router has not determined the virtual IP address and has not yet seen an authenticated message from the active router. In this state the router is still waiting to hear from the active router.
- If the state is 'Listen' then it indicates that the router knows the virtual IP address but is neither the active router nor the standby router. It listens for messages from those routers.
- If the state is 'Speak' then it indicates the router is actively participating in the election of the active and/or standby router. A router cannot enter Speak state unless it has the virtual IP address.
- If the state is 'Standby' then it indicates the router is a candidate to become the next active router and sends periodic messages. Excluding transient conditions, there MUST be at most one router in the group in Standby state.
- If the state is 'Active' then it indicates the router is currently forwarding packets that are sent to the group's virtual MAC address.

Diagnostic Commands:

To display Hot Standby Router Protocol (HSRP) information, use the show standby command in privileged EXEC mode.

show standby [*type number* [*group-number*]] [active | init | listen | standby] [brief]

type number	(Optional) Interface type and number for which output is displayed.
group number	(Optional) Group number on the interface for which output is displayed.
active	(Optional) Displays HSRP groups in the active state.
init	(Optional) Displays HSRP groups in the initial state.
listen	(Optional) Displays HSRP groups in the listen or learn state.
standby	(Optional) Displays HSRP groups in the standby or speak state.
brief	(Optional) Summarizes each standby group as a single line of output.

Go Top

SECTION 4.81

Trap: ciscoFlashCopyCompletionTrap

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FlashCopyCompletion	Trap	Event	No	Informational	Flash copy operation complete on $NodeDisplayName. Status: $ciscoFlashCopyStatus.	FlashCopyCompletion	Common

Description:

A ciscoFlashCopyCompletionTrap is sent at the completion of a flashcopy operation if such a trap was requested when the operation was initiated.

Default Message:

Flash copy operation complete on $NodeDisplayName. Status: $ciscoFlashCopyStatus.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
	The status of the specified copy operation. • copyOperationPending (0) - An operation request is received and pending for validation and process • copyInProgress (1) - The specified operation is active • copyOperationSuccess (2) - The specified operation is supported and completed successfully • copyInvalidOperation (3) - Command is invalid or command-protocol-device combination is unsupported

ciscoFlashCopyStatus	copyInvalidProtocol (4) - An invalid protocol is specified • copyInvalidSourceName (5) - An invalid source file name is specified. For the copy from flash to lex operation, this error code will be returned when the source file is not a valid lex image. • copyInvalidDestName (6) - An invalid target name (file or partition or device name) is specified • copyInvalidServerAddress (7) - An invalid server address is specified • copyDeviceBusy (8) - The specified device is in use or locked by another process • copyDeviceOpenError (9) - An invalid device name is specified • copyDeviceError (10) - A device read, write or erase error occurred • copyDeviceNotProgrammable (11) - The device is read-only but a write or erase operation is specified • copyDeviceFull (12) - The device is filled to capacity • copyFileOpenError (13) - An invalid file name or file not found in partition • copyFileTransferError(14) - File transfer is unsuccessful or network failure • copyFileChecksumError(15) - File checksum in Flash failed • copyNoMemory (16) - System is running low on memory • copyUnknownFailure(17) - Failure unknown • copyInvalidSignature(18) - An invalid signature is specified

Operational Information:

- This is an informational trap indicating the status of a flash copy operation.

Go Top

SECTION 4.82

Trap: ciscoFlashPartitioningCompletionTrap

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FlashPartitioningCompletion	Trap	Event	No	Informational	Flash partitioning operation complete on $NodeDisplayName. Status: $ciscoFlashPartitioningStatus.	FlashPartitioningCompletion	Common

Description:

A ciscoFlashPartitioningCompletionTrap is sent at the completion ofa partitioning operation if such a trap was requested when the operation was initiated.

Default Message:

Flash partitioning operation complete on $NodeDisplayName. Status: $ciscoFlashPartitioningStatus.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
	The status of the specified partitioning operation: • partitioningInProgress (1) - The specified operation is active • partitioningOperationSuccess (2) - The specified operation is supported and completed successfully • partitioningInvalidOperation (3) - Command is invalid or command-protocol-device combination is unsupported

ciscoFlashPartitioningStatus	partitioningInvalidDestName (4) - An invalid target name (file or partition or device name) is specified • partitioningInvalidPartitionCount (5) - An invalid partition count specified for the partitioning command • partitioningInvalidPartitionSizes (6) - An invalid partition size, or invalid count of partition sizes • partitioningDeviceBusy (7) - The specified device is in use or locked by another process • partitioningDeviceOpenError (8) - An invalid device name was specified • partitioningDeviceError (9) - A device read, write or erase error occurred • partitioningNoMemory (10) - System is running low on memory • partitioningUnknownFailure (11) - Failure unknown

Operational Information:

- This is an informational trap indicating the status of a partition flash operations.

Go Top

SECTION 4.83

Trap: ciscoFlashMiscOpCompletionTrap

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FlashMiscOpCompletion	Trap	Event	No	Informational	Flash miscellaneous operation complete on $NodeDisplayName. Status: $ciscoFlashMiscOpStatus.	FlashMiscOpCompletion	Common

Description:

A ciscoFlashMiscOpCompletionTrap is sent at the completion of amiscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.

Default Message:

Flash miscellaneous operation complete on $NodeDisplayName. Status: $ciscoFlashMiscOpStatus.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ciscoFlashMiscOpStatus	The status of the specified copy operation. • miscOpInProgress (1) - The specified operation is active • miscOpOperationSuccess (2) - The specified operation is supported and completed successfully • miscOpInvalidOperation (3) - Command is invalid or command-protocol-device combination is unsupported • miscOpInvalidDestName (4) - An invalid target name (file or partition or device name) is specified • miscOpDeviceBusy (5) - The specified device is in use or locked by another process • miscOpDeviceOpenError (6) - An invalid device name was specified • miscOpDeviceError (7) - A device read, write or erase error occurred • miscOpDeviceNotProgrammable (8) - The device is read-only but a write or erase operation is specified • miscOpFileOpenError (9) - An invalid file name or file not found in partition • miscOpFileDeleteFailure (10) - A file could not be deleted or delete count exceeded

	miscOpFileUndeleteFailure (11) - A file could not be un-deleted or un-delete count exceeded • • miscOpFileChecksumError(12) - File has a bad checksum • miscOpNoMemory (13) - System is running low on memory • miscOpUnknownFailure(14) - Failure unknown • miscOpSqueezeFailure(15) - The squeeze operation failed • miscOpNoSuchFile(16) - A valid but non-existent file name was specified • miscOpFormatFailure(17) - The format operation failed

Operational Information:

- This is an informational trap indicating the status of a misc flash operations.

Go Top

SECTION 4.84

Trap: cefcFRUInserted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FRU	Trap	Event	No	Normal	A field replaceable unit was inserted on $NodeDisplayName. Description: $entPhysicalDescr	FRU	Common
FRU	Trap	Event	No	Major	A field replaceable unit was removed on $NodeDisplayName. Description: $entPhysicalDescr	FRU	Common

Description:

The cecfFRUInserted notification indicates that aFRU was inserted. The varbind for this notification indicates the entPhysicalIndex of the inserted FRU, and the entPhysicalIndex of the FRU's container.

Default Message:

A field replaceable unit was inserted on $NodeDisplayName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
entPhysicalContainedIn	The value of entPhysicalIndex for the physical entity which 'contains' this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity. Note that the set of 'containment' relationships define a strict hierarchy; that is, recursion is not allowed. In the event a physical entity is contained by more than one physical entity (e.g., double-wide modules), this object should identify the containing entity with the lowest value of entPhysicalIndex.

Operational Information:

- A new field replaceable unit such as line cards, fan, port, power supply or redundant power supply was added. No action is required.

Go Top

SECTION 4.85

Trap: clogMessageGenerated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SyslogEvent	Trap	Event	No	Critical	$NodeDisplayName ($NodeSerialNum) - $Facility-$MsgName:$MsgText.	SyslogEvent	Common
SyslogEvent	Trap	Event	No	Critical	$NodeDisplayName ($NodeSerialNum) - $Facility-$MsgName:$MsgText.	SyslogEvent	Common
SyslogEvent	Trap	Event	No	Major	$NodeDisplayName ($NodeSerialNum) - $Facility-$MsgName:$MsgText.	SyslogEvent	Common
SyslogEvent	Trap	Event	No	Minor	$NodeDisplayName ($NodeSerialNum) - $Facility-$MsgName:$MsgText.	SyslogEvent	Common
SyslogEvent	Trap	Event	No	Warning	$NodeDisplayName ($NodeSerialNum) - $Facility-$MsgName:$MsgText.	SyslogEvent	Common
SyslogEvent	Trap	Event	No	Warning	$NodeDisplayName ($NodeSerialNum) - $Facility-$MsgName:$MsgText.	SyslogEvent	Common
SyslogEvent	Trap	Event	No	Informational	$NodeDisplayName ($NodeSerialNum) - $Facility-$MsgName:$MsgText.	SyslogEvent	Common
SyslogEvent	Trap	Event	No	Informational	$NodeDisplayName ($NodeSerialNum) - $Facility-$MsgName:$MsgText.	SyslogEvent	Common

Description:

When a syslog message is generated by the device a clogMessageGeneratednotification is sent. The sending of these notifications can be enabled/disabled via the clogNotificationsEnabled object.

Default Message:

$NodeDisplayName ($NodeSerialNum) - $Facility-$MsgName:$MsgText.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
Facility	Name of the facility that generated this message. For example: 'SYS'.
Severity	The severity of a syslog message. The enumeration values are equal to the values that syslog uses + 1. For example, with syslog, emergency=0. • 'emergency' (1) : system is unusable • 'alert' (2) : action must be taken immediately • 'critical' (3) : critical conditions • 'error' (4) : error conditions • 'warning' (5) : warning conditions • 'notice' (6) : normal but significant condition • 'informational' (7) : informational messages • 'debug' (8) : debug-level messages
MsgName	A textual identification for the message type. A facility name in conjunction with a message name uniquely identifies a message type.
MsgText	The text of the message. If the text of the message exceeds 255 bytes, the message will be truncated to 254 bytes and a '*' character will be appended - indicating that the message has been truncated.
Timestamp	The value of sysUpTime when this message was generated.

Operational Information:

- This trap can indicate many things. The MsgName and MsgText can provide more information related on the probable cause of this notification.
- It can indicate a link error or increased link utilization. It can also indicate increase in device CPU or memory utilization. You can investigate further depending on the message log.

See Also:

ciscoEnvMonTemperatureNotification Trap
ciscoProducts Trap
ciscoGspLinkStateChange Trap
ciscoGspCongestionChange Trap

cefcModuleStatusChange Trap

Go Top

SECTION 4.86

Trap: ciscoAuthenticationFailure and authenticationFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AuthenticationFailure	Trap	Event	No	Major	$NodeDisplayName - authentication failure. $authAddr is accessing this device via wrong community string.	AuthenticationFailure	Common
AuthenticationFailure	Trap	Event	No	Major	$NodeDisplayName - authentication failure. $authAddr is accessing this device via wrong community string.	AuthenticationFailure	Common

Description:

A ciscoAuthenticationFailure trap signifies that the SNMP entity has received aprotocol message that is not properly authenticated. You get this trap if a network management system (NMS) polls the device with the wrong community string.

ciscoAuthenticationFailure replaces the old authenticationFailure trap.

Default Message:

- $NodeDisplayName - authentication failure. $authAddr is accessing this device via wrong community string.

Message Substitution Variables:

authAddr	This is the last SNMP authorization failure IP address.

Operational Information:

- If $authAddr is a valid system that should poll the device, you need toinvestigate the system in order to determine why the system uses the wrong community. Then, change the system to the correct community string.
- If the system is not a known NMS, the problem can be that something istrying to hack into the device via SNMP.
- You can also check for crash files on bootflash: or flash: filesystems

Diagnostic Commands:

- The community information, is displayed in the running config. Run the 'show running-config | include community' command in privileged EXEC mode.
- In MWTM, the community information can seen using the MWTM - Node SNMP and Credentials Editor

Go Top

SECTION 4.87

Trap: chassisAlarmOn

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChassisAlarm	Trap	Event	No	Major	$NodeDisplayName -- Chassis alarms reported: Chassis major alarm is $chassisMajorAlarm, Chassis minor alarm is $chassisMinorAlarm, Chassis temperature alarm is $chassisTempAlarm	ChassisAlarm	Common
ChassisAlarm	Trap	Event	No	Normal	$NodeDisplayName -- Chassis alarms reported: Chassis major alarm is off, Chassis minor alarm is off, Chassis temperature alarm is off	ChassisAlarm	Common
ChassisAlarm	Trap	Event	No	Major	$NodeDisplayName -- Chassis alarms reported: Chassis major alarm is $chassisMajorAlarm, Chassis minor alarm is $chassisMinorAlarm, Chassis temperature alarm is $chassisTempAlarm	ChassisAlarm	Common

Description:

A chassisAlarmOn trap signifies that the agent entity has detected the chassisTempAlarm, chassisMinorAlarm, or chassisMajorAlarm object in this MIB has transitioned to the on(2) state. The generation of this trap can be controlled by the sysEnableChassisTraps object in this

MIB.

Default Message:

$NodeDisplayName -- Chassis alarms reported: Chassis major alarm is $chassisMajorAlarm, Chassis minor alarm is $chassisMinorAlarm, Chassis temperature alarm is $chassisTempAlarm

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
chassisTempAlarm	The chassis temperature alarm status. The possible states are: • off • on • critical
chassisMinorAlarm	The chassis minor alarm status. The possible states are: • off • on
chassisMajorAlarm	The chassis major alarm status. The possible states are: • off • on

Operational Information:

- If the chassis temperature is too high, a minor or major alarm can be generated. You can inspect the indicated component closely to determine why it is operating out of the normal operating temperature range and whether it will eventually exceed the allowed operating temperature range.
- This alarm can indicate a redundant power supply has been powered off. You may want to replace the FRU.
- This alarm can also indicate that one or more fans in the system fan tray have failed. You can replace the system fan tray to fix the problem.

Diagnostic Commands:

To display system status information "show environment" command in privileged EXEC mode.

show environment [alarm | cooling | status | temperature | voltage]

alarm	(Optional) Displays environmental alarms. • status - Displays alarm status. • thresholds - Displays alarm thresholds
cooling	(Optional) Displays fan tray status, chassis cooling capacity, ambient temperature, and per-slot cooling capacity.
status	(Optional) Displays FRU operational status with power and temperature information.
temperature	(Optional) Displays FRU temperature information.
voltage	(Optional) Displays FRU voltage information.

Go Top

SECTION 4.88

Trap: cempMemBufferNotify

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MemBufferNotify	Trap	Event	No	Informational	$NodeDisplayName -- The peak value for buffer pool $cempMemBufferName was updated to $cempMemBufferPeak.	MemBufferNotify	Common

Description:

```
Whenever cempMemBufferPeak object is updated in the        buffer pool, a cempMemBufferNotify notification
is sent. The sending of these notifications can be
enabled/disabled via the cempMemBufferNotifyEnabled object.
```

Default Message:

$NodeDisplayName -- The peak value for buffer pool $cempMemBufferName was updated to $cempMemBufferPeak.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cempMemBufferName	A textual name assigned to the buffer pool. This object is suitable for output to a human operator, and may also be used to distinguish among the various buffer types. For example: 'Small', 'Big', 'Serial0/1' etc.
cempMemBufferPeak	Indicates the peak number of buffers in pool on the physical entity.
cempMemBufferPeakTime	Indicates the time of most recent change in the peak number of buffers (cempMemBufferPeak object) in the pool.

Go Top

SECTION 4.89

Trap: ciscoICsuDsuT1LoopStatusNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Loopback	Trap	Event	No	Informational	$NodeDisplayName -- Line placed in loopback from remote. Index=placedInLoopback[2]	Loopback	Common
Loopback	Trap	Event	No	Informational	$NodeDisplayName -- Line taken out of loopback from remote. Index=placedInLoopbackCleared[2]	Loopback	Common
Loopback	Poll	Event	No	Informational	$NodeDisplayName $ifDescr Line taken out of loopback from remote.	Loopback	Common
Loopback	Poll	Event	No	Informational	$NodeDisplayName $ifDescr Line placed in loopback from remote.	Loopback	Common

Description:

```
Indicates a change in T1 Loop Status.
```

Default Message:

$NodeDisplayName -- (AIS, blue alarm) Indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (AIS, blue alarm cleared) The transmission interruption has cleared. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm) The transmitting equipment has lost its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (RAI, yellow alarm cleared) The transmitting equipment has recovered its incoming signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF) Unable to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOF cleared) Able to synchronize on the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- Line placed in loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]

$NodeDisplayName -- Line taken out of loopback from remote. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS) Unable to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]
$NodeDisplayName -- (LOS cleared) Able to detect the DS1 signal. Index=$ciscoICsuDsuT1LoopStatus[2]

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
ciscoICsuDsuT1LoopStatus	Current Loop status of T1 CSU/DSU. Represented as a sum of a bit map. The variable bit positions are: 1 - lossofSignal (LOS); unable to detect the DS1 signal. 2 - lossofFrame (LOF); unable to synchronize on the DS1 signal. 4 - detectedRemoteAlarmIndication (RAI); indicates that the transmitting equipment has lost its incoming signal. RAI is commonly called yellow alarm. 8 - detectedAlarmIndicationSignal (AIS); indicates that there is a transmission interruption located either at the equipment originating the AIS signal or upstream of that equipment. Indicated by an unframed, all-'ones' signal. Also known as blue alarm. 16 - placedInLoopback; Line placed in loopback from remote.

Go Top

SECTION 4.90

Trap: cEventMgrServerEvent

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EEM-ServerEvent	Trap	Event	No	Informational	$NodeDisplayName - EEM event - EEM Policy name: $ceemHistoryPolicyName	EEM-ServerEvent	Common

Description:

This notification is sent by the Embedded Event Manager server after it has run a policy associated with the event ceemHistoryEventType that was received.

Default Message:

$NodeDisplayName - EMM Policy event - Policy Name: $ceemHistoryPolicyName. Policy String Data: $ceemHistoryPolicyStrData

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ceemHistoryEventType1	The type of Embedded Event Manager event which was detected. The value corresponds to an entry in the ceemEventTable.
ceemHistoryEventType2	The type of Embedded Event Manager event which was detected. The value corresponds to an entry in the ceemEventTable.
ceemHistoryEventType3	The type of Embedded Event Manager event which was detected. The value corresponds to an entry in the ceemEventTable.
ceemHistoryEventType4	The type of Embedded Event Manager event which was detected. The value corresponds to an entry in the ceemEventTable.
ceemHistoryPolicyPath	The file path on the router where the Embedded Event Manager policy that was triggered is stored. If the size of the file path string is larger than 128, the end characters will be truncated.
ceemHistoryPolicyName	The name of the Embedded Event Manager policy that was triggered because of an Embedded Event Manager event. The name must be a valid Embedded Event Manager policy name. It must be in the form of a valid Posix filename.
ceemHistoryPolicyExitStatus	The exit status of the Embedded Event Manager policy execution. This value corresponds to the Posix process exit status.
ceemHistoryEventIndex	A monotonically increasing non-zero integer uniquely identifying a generated event. When it reaches the maximum value, the agent wraps the value back to 1 and may flush all existing entries in the event table.

Go Top

Trap: cEventMgrPolicyEvent

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EEM-PolicyEvent	Trap	Event	No	Informational	$NodeDisplayName - EEM Policy event - Policy Name: $ceemHistoryPolicyName. Policy String Data: $ceemHistoryPolicyStrData	EEM-PolicyEvent	Common

Description:

This notification is configured to be sent from within an Embedded Event Manager policy after an Embedded Event Manager event ceemHistoryEventType has occurred.

Default Message:

$NodeDisplayName - EMM event - EMM Policy name: $ceemHistoryPolicyName

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ceemHistoryEventType1	The type of Embedded Event Manager event which was detected. The value corresponds to an entry in the ceemEventTable.
ceemHistoryEventType2	The type of Embedded Event Manager event which was detected. The value corresponds to an entry in the ceemEventTable.
ceemHistoryEventType3	The type of Embedded Event Manager event which was detected. The value corresponds to an entry in the ceemEventTable.
ceemHistoryEventType4	The type of Embedded Event Manager event which was detected. The value corresponds to an entry in the ceemEventTable.
ceemHistoryPolicyPath	The file path on the router where the Embedded Event Manager policy that was triggered is stored. If the size of the file path string is larger than 128, the end characters will be truncated.
ceemHistoryPolicyName	The name of the Embedded Event Manager policy that was triggered because of an Embedded Event Manager event. The name must be a valid Embedded Event Manager policy name. It must be in the form of a valid Posix filename.
ceemHistoryPolicyIntData1	Arbitrary integer data that the Embedded Event Manager policy can use. Use of this object is optional. If unused by a policy, this object will not be instantiated for that policy.
ceemHistoryPolicyIntData2	Arbitrary integer data that the Embedded Event Manager policy can use. Use of this object is optional. If unused by a policy, this object will not be instantiated for that policy.
ceemHistoryPolicyStrData	Arbitrary string data the Embedded Event Manager policy can use. Use of this object is optional. If unused by a policy, this object will not be instantiated for that policy.
ceemHistoryEventIndex	A monotonically increasing non-zero integer uniquely identifying a generated event. When it reaches the maximum value, the agent wraps the value back to 1 and may flush all existing entries in the event table.

Go Top

Trap: tcpConnectionClose

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
TcpConnectionClose	Trap	Event	No	Warning	$NodeDisplayName - user logged in/out of the device from $tcpConnState_tcpConnRemAddress	TcpConnectionClose	Common

Description:

```
A tty trap signifies that a TCP connection,                    previously established with the sending
protocol entity for the purposes of a tty
session, has been terminated.
```

Default Message:

$NodeDisplayName - user logged in/out of the device from $tcpConnState_tcpConnRemAddress.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
tslineSesType	Type of session. INTEGER is unknown
tcpConnState	The state of this TCP connection. The only value which may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the TCB (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably). INTEGER is unknown
loctcpConnElapsed	How long this TCP connection has been established.
loctcpConnInBytes	Bytes input for this TCP connection.
loctcpConnOutBytes	Bytes output for this TCP connection.
tsLineUser	TACACS user name, if TACACS enabled, of user on this line.
tcpConnLocalAddress	The local IP address for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.
tcpConnLocalPort	The local port number for this TCP connection.
tcpConnRemPort	The remote port number for this TCP connection.
tslineSesLine	Table index 1.
tcpConnRemAddress	The remote IP address for this TCP connection.
tslineSesSession	Table index 2.
tsLineNumber	The line i've been talking about.

Go Top

SECTION 4.93

Trap: cefInconsistencyDetection

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CefInconsitencyState	Trap	Event	No	Informational	$NodeDisplayName - CEF consistency checker detects an inconsistent prefix in one of the CEF forwarding databases.	CefInconsitencyState	Common

Description:

```
A cefInconsistencyDetection notification is generated          when CEF consistency checkers detects an inconsistent
prefix in one of the CEF forwarding databases.
Note that the generation of cefInconsistencyDetection
notifications is throttled by the agent, as specified
by the 'cefNotifThrottlingInterval' object.
```

Default Message:

$NodeDisplayName - CEF consistency checker detects an inconsistent prefix in one of the CEF forwarding databases.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
entLastInconsistencyDetectTime	The value of sysUpTime at the time an inconsistency is detecetd.

Go Top

SECTION 4.94

Trap: cefPeerFIBStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CefPeerFIBState	Trap	Event	No	Critical	$NodeDisplayName - Cef Peer Entity FIB Operational state is down.	CefPeerFIBState	Common
CefPeerFIBState	Trap	Event	No	Informational	$NodeDisplayName - Cef Peer Entity FIB reload request is raised.	CefPeerFIBState	Common
CefPeerFIBState	Trap	Event	No	Informational	$NodeDisplayName - Cef Peer Entity FIB is reloading.	CefPeerFIBState	Common
CefPeerFIBState	Trap	Event	No	Informational	$NodeDisplayName - Cef Peer Entity FIB is synchronized.	CefPeerFIBState	Common
CefPeerFIBState	Trap	Event	No	Normal	$NodeDisplayName - Cef Peer Entity FIB Operational state is up.	CefPeerFIBState	Common

Description:

```
A cefPeerFIBStateChange notification is generated if          change in cefPeerFIBOperState is detected for the
peer entity.
```

Default Message:

cefPeerFIBOperState :
1. peerFIBDown :
$NodeDisplayName - Cef Peer Entity $entPhysicalDescr FIB Operational state is down.
2. peerFIBReloadRequest :
$NodeDisplayName - Cef Peer Entity $entPhysicalDescr FIB reload request is raised.
3. peerFIBReloading :
$NodeDisplayName - Cef Peer Entity $entPhysicalDescr FIB is reloading.
4. peerFIBSynced :
$NodeDisplayName - Cef Peer Entity $entPhysicalDescr FIB is synchronized.
5. peerFIBUp :
$NodeDisplayName - Cef Peer Entity $entPhysicalDescr FIB Operational state is up.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router

	that sent the trap.
entPhysicalDescr	A textual description of physical entity. This object should contain a string which identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.
cefPeerFIBOperState	The current CEF FIB Operational State for the CEF peer entity. INTEGER is unknown
entPhysicalIndex	The index for this entry.
entPeerPhysicalIndex	The entity index for the CEF peer entity. Only the entities of 'module' entPhysicalClass are included here.
cefFIBIpVersion	The version of IP forwarding.

Go Top

SECTION 4.95

Trap: cefPeerStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CefPeerState	Trap	Event	No	Critical	$NodeDisplayName - Cef Peer Entity encounters a fatal error.	CefPeerState	Common
CefPeerState	Trap	Event	No	Normal	$NodeDisplayName - Cef Peer Entity is up.	CefPeerState	Common
CefPeerState	Trap	Event	No	Warning	$NodeDisplayName - Cef Peer Entity is in the hold stage.	CefPeerState	Common

Description:

```
A cefPeerStateChange notification is generated if         change in cefPeerOperState is detected for the
peer entity.
```

Default Message:

cefPeerOperState :
1. peerDisabled :
$NodeDisplayName - Cef Peer Entity $entPhysicalDescr encounters a fatal error.
2. peerUp :
$NodeDisplayName - Cef Peer Entity $entPhysicalDescr is up.
3. peerHold :
$NodeDisplayName - Cef Peer Entity $entPhysicalDescr is in the held stage.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
entPhysicalDescr	A textual description of physical entity. This object should contain a string which identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.
cefPeerOperState	The current CEF operational state of the CEF peer entity. Cef peer entity oper state will be peerDisabled(1) in the following condition: : Cef Peer entity encounters fatal error i.e. resource allocation failure, ipc failure etc : When a reload/delete request is received from the Cef Peer Entity

	Once the peer entity is up and no fatal error is encountered, then the value of this object will transits to the peerUp(3) state. If the Cef Peer entity is in held stage, then the value of this object will be peerHold(3). Cef peer entity can only transit to peerDisabled(1) state from the peerHold(3) state. INTEGER is unknown
entPhysicalIndex	The index for this entry.
entPeerPhysicalIndex	The entity index for the CEF peer entity. Only the entities of 'module' entPhysicalClass are included here.

Go Top

SECTION 4.96

Trap: cefResourceFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ExpFwdResourceFailure	Trap	Event	No	Warning	$NodeDisplayName - CEF resource failed due to $cefResourceFailureReason.	ExpFwdResourceFailure	Common

Description:

```
A cefResourceFailure notification is generated when          CEF resource failure on the managed entity is
detected. The reason for this failure is indicated
by cefResourcefFailureReason.
```

Default Message:

$NodeDisplayName - CEF resource failed on the entity $entPhysicalDescr due to $cefResourceFailureReason.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
entPhysicalDescr	A textual description of physical entity. This object should contain a string which identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.
cefResourceFailureReason	The CEF resource failure reason which may lead to CEF being disabled on the managed entity. Reason of CEF Failure: none(1) : no failure mallocFailure(2) : memory allocation failed for CEF hwFailure(3) : hardware interface failure for CEF keepaliveFailure(4) : keepalive was not received from the CEF peer entity noMsgBuffer(5) : message buffers were exhausted while preparing IPC message to be sent to the CEF peer entity invalidMsgSize(6) : IPC message was received with invalid size from the CEF peer entity internalError(7) : Some other internal error was detected for CEF
entPhysicalIndex	The index for this entry.

Go Top

Trap: ceAlarmAsserted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EntityAlarmAsserted	Trap	Event	No	Warning	$NodeDisplayName - The Physical entity asserts a $ceAlarmHistSeverity alarm.	EntityAlarmAsserted	Common
EntityAlarmAsserted	Trap	Event	No	Normal	$NodeDisplayName - The Physical entity clears the previously asserted alarm of $ceAlarmHistSeverity severity.	EntityAlarmAsserted	Common

Description:

```
The agent generates this trap when a physical entity        asserts an alarm.
```

Default Message:

$NodeDisplayName - The Physical entity $entPhysicalDescr asserts a $ceAlarmHistSeverity alarm of type $ceAlarmHistAlarmType.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
entPhysicalDescr	A textual description of physical entity. This object should contain a string which identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.
ceAlarmHistSeverity	This object specifies the severity of the alarm generated. Each alarm type defined by a vendor type employed by the system has an associated severity. Bellcore TR-NWT-000474 defines these severities as follows: 'critical' An alarm used to indicate a severe, service-affecting condition has occurred and that immediate corrective action is imperative, regardless of the time of day or day of the week. 'major' An alarm used for hardware or software conditions that indicate a serious disruption of service or the malfunctioning or failure of important hardware. These troubles require the immediate attention and response of a technician to restore or maintain system capability. The urgency is less than in critical situations because of a lesser immediate or impending effect on service or system performance. 'minor' An alarm used for troubles that do not have a serious effect on service to customers or for troubles in hardware that are not essential to the operation of the system. 'info' An indication used to raise attention to a condition that could possibly be an impending problem or to notify the customer of an event that improves operation.
ceAlarmHistEntPhysicalIndex	This object specifies the physical entity that generated the alarm.
ceAlarmHistAlarmType	This object specifies the type of alarm generated.
ceAlarmHistTimeStamp	This object specifies the value of the sysUpTime object at the time the alarm was generated.

ceAlarmHistIndex	An integer value uniquely identifying the entry in the table. The value of this object starts at '1' and monotonically increases for each alarm condition transition monitored by the agent. If the value of this object is '4294967295', the agent will reset it to '1' upon monitoring the next alarm condition transition.

Go Top

SECTION 4.98

Syslog : Syslog

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Syslog	Syslog	Event	No	Warning	$NodeDisplayName - Syslog message received.	Syslog	Common

Go Top

SECTION 4.99

Status: NodeStateAdded and NodeStateChanged

Description:

The NodeStateAdded and NodeStateChanged status events provide information when a Node object is added to the MWTM object model or when MWTM detects that the state of a Node has changed. The value of NodeState indicates the new state. Possible values of NodeState include:

- Active - The Node is fully functional.
- Unknown - An attempt was made to poll the Node but there was an error in polling.
- Warning - The Node has been polled and traffic may or may not be running. Check the state reason and the status of the interfaces carrying traffic.
- Unmanaged - The Node is not pollable.
- Waiting - The Node is scheduled to be polled but the poll has not started.
- Discovering - The Node is being discovered via a poll.
- Polling - The Node is in the process of being polled.

Default Message:

- Node $NodeDisplayName added in state $NodeState/$NodeStateReason.
- Node $NodeDisplayName changed state from $NodeLastState to $NodeState/$NodeStateReason.

Message Substitution Variables:

of the Node.

Node	Substitution variables for Node related data.
NodeState	The current state of the Node.
NodeStateReason	The current state reason of the Node.
NodeLastState	The previous state of the Node.

Operational Information:

- If the current state of the Node is Active no additional action is necessary.
- If the current state of the Node is Unknown this is an indication that one of several events has occurred. Check the Node Details for the Node in question for the following problems.
  - A SNMP Timeout has occurred trying to poll the router due to an invalid SNMP community string specification in which case you can reset the community string in the MWTM Node SNMP and Credentials Editor.
  - A SNMP Timeout has occurred because of a network failure in which case you should have your IP administrator check on the network status.
  - A SNMP Timeout has occurred because of a low bandwidth network connection. In this situation you can adjust the SNMP timeout values for Node in the MWTM Node SNMP and Credentials Editor.
  - SNMP is a low priority task on the router and as such if the router is excessively busy with other functions will not reply to the SNMP poll request in a timely manner. In this case the next poll may succeed when the activity on the router clears or you can adjust the SNMP timeout values for Node in the MWTM Node SNMP and Credentials Editor.
  - A SNMP Error has occurred in which case you should contact MWTM support personnel. The MWTM Message log may have more information relating to the

problem.

- If the current state of the Node is Warning this is an indication that one of the node's RtrInterfaces has a problem.
- If the current state of the Node is Unmanaged this is an indication that MWTM is unable to poll this device due to one of the following reasons.
  - The node is known indirectly by MWTM. In other words, MWTM knows the device exists but there is no known SNMP stack on the device for MWTM to query.
  - During recursive discovery MWTM discovers all seed nodes and attempts to manage them, then flags all nodes that are adjacent to those seed nodes as Unmanaged
  - A MWTM user has set the node to Unmanaged status, to prevent MWTM from polling the node for status or statistical information.
- When the current state of the Node is Waiting the node is in a queue waiting to be polled during the MWTM discovery process. This state should only be seen when a discovery is in process.
- When the current state of the Node is Discovering the node has been removed from the waiting to be polled queue and is actively being polled. This state should only be seen when a discovery is in process.
- When the current state of the Node is Polling a MWTM user has specifically requested a poll of this Node.

Go Top

SECTION 4.100

Status: SnmpTimeout

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SnmpTimeout	Poll	Event	No	Warning	An SNMP timeout occurred polling $NodeDisplayName address $FailedPollAddress. Retrying $NextPollAddress .	SnmpTimeout	Common
SnmpTimeout	Poll	Event	No	Major	An SNMP timeout occurred polling $NodeDisplayName address $FailedPollAddress. No interfaces available for retry.	SnmpTimeout	Common

Description:

The SnmpTimeout status event provides information when MWTM detects that a poll of a Node has timed out. MWTM will retry the poll to a Node on another interface if it has multiple interfaces defined to MWTM as being SNMPable. The value of NextInterface indicates if there is another interface to retry the poll on or not.

Default Message:

- An SNMP timeout occurred polling $NodeDisplayName address $FailedPollAddress. Retrying $NextPollAddress.
- An SNMP timeout occurred polling $NodeDisplayName address $FailedPollAddress. No interfaces available for retry.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
NextInterface	True or False indicating if a NextPollAddress exists.
FailedPollAddress	The IP address of the interface that the poll timed out on.
NextPollAddress	The IP address of the interface that MWTM will retry the poll on.

Operational Information:

- The common reason may be due to an invalid SNMP community string specification in which case you can reset the community string in the MWTM Node SNMP and Credentials Editor.
- A timeout can occur because of a network failure in which case you should have your IP administrator check on the network status.
- A timeout can also occur because of a low bandwidth network connection. In this situation you can adjust the SNMP timeout values for Node in MWTM Node SNMP and Credentials Editor.
- Additionally you can also see the description of the#nodeUnknown Unknown state for a Node for other possible causes.

Go Top

SECTION 4.101

Status: SGMError

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApplicationError	Poll	Event	No	Minor	A nonFatal error occured in $Module. $ErrorString	ApplicationError	Common
ApplicationError	Poll	Event	No	Major	A Fatal error occured in $Module. $ErrorString	ApplicationError	Common

Description:

The SGMError status event provides information when MWTM experiences an unexpected error during Processing. The value of SGMErrorType indicates the type of error. Possible values of SGMErrorType include:

- nonFatal - SGM server processing continues.
- Fatal - SGM server processing terminates.

Default Message:

A $SGMErrorType error occurred in $Module. $ErrorString

Message Substitution Variables:

SGMErrorType	Indicates the type of error that occurred. Either nonFatal or Fatal.
Module	Indicates the MWTM server module that the error occurred in.
ErrorString	A detailed error message describing the error.

Operational Information:

- When SGMErrorType is nonFatal server processing continues. However functionality may be degraded.
- When SGMErrorType is Fatal the SGM server will terminate. A restart may or may not be automatically performed depending on the nature of the error.
- If error persists, you can also contact MWTM personnel along with 'mwtm tac' output

Go Top

SECTION 4.102

Status: GroupStateAdded and GroupStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GroupState	Poll	Event	No	Normal	Group $GroupDisplayName added in state Active/ActiveReason.	GroupState	Common
GroupState	Poll	Event	No	Warning	Group $GroupDisplayName added in state Warning/WarningReason.	GroupState	Common
GroupState	Poll	Event	No	Warning	Group $GroupDisplayName added in state Unknown/UnknownReason.	GroupState	Common
GroupState	Poll	Event	No	Informational	Group $GroupDisplayName added in state $GroupState/$GroupStateReason.	GroupState	Common
GroupState	Poll	Event	No	Normal	Group $GroupDisplayName changed state from $GroupLastState to Active/ActiveReason.	GroupState	Common
GroupState	Poll	Event	No	Warning	Group $GroupDisplayName changed state from $GroupLastState to Warning/WarningReason.	GroupState	Common
GroupState	Poll	Event	No	Warning	Group $GroupDisplayName changed state from $GroupLastState to Unknown/UnknownReason.	GroupState	Common
GroupState	Poll	Event	No	Informational	Group $GroupDisplayName changed state from $GroupLastState to $GroupState/$GroupStateReason.	GroupState	Common

Description:

The GroupStateAdded and GroupStateChanged status eventsprovide information when a Group object is added to the MWTM object model or when MWTM detects that the state of a Group has changed. The value of GroupState indicates the new state.
Possible values of GroupState include:

- Active - Traffic may flow over this Group.
- Unknown - The attempt to determine the state of the Group failed.
- Warning - The Group is Active however some underlying interface of this Group is not fully functional.
- Failed - All underlying interfaces are not functional.
- Deleted - The Group has been deleted from the object database.

Default Message:

- Group $GroupDisplayName added in state $GroupState/$GroupStateReason.

- Group $GroupDisplayName changed state from $GroupLastState to $GroupState/$GroupStateReason.

Message Substitution Variables:

GroupDisplayName	The name of the Group.
GroupState	The current state of the Group.
GroupStateReason	The current state reason of of the Group.
GroupLastState	The previous state of the Group.

Operational Information:

See also:

Go Top

SECTION 4.103

UserAction: NodeIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NodeIgnoredSet	User Action	Event	No	Informational	Node $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.	NodeIgnoredSet	Common

Description:

The NodeIgnored UserAction event provides information when a Node's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the Node in the aggregation algorithm in determining the state of a View. The value of IgnoredFlag indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The node is to be excluded from state aggregation.
- False - The node is to be included in state aggregation.

Default Message:

Node $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node	
Substitution variables for Node related data.	
NodeState	The current state of the Node.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the nodes which are currently ignored select Node folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 4.104

UserAction: RtrInterfaceIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RtrInterfaceIgnoredSet	User Action	Event	No	Informational	Interface $NodeDisplayName/$RtrInterfaceDisplayName ignore flag is set to $IgnoredFlag by $User.	RtrInterfaceIgnoredSet	Common

Description:

The RtrInterfaceIgnored UserAction event provides information when a RtrInterface's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the RtrInterface in the aggregation algorithm in determining the state of a View. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The node is to be excluded from state aggregation.
- False - The node is to be included in state aggregation.

Default Message:

Interface $NodeDisplayName/$RtrInterfaceDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
RtrInterfaceState	The current state of the RtrInterface.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Go Top

SECTION 4.105

UserAction: NodeProcessTrapsSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NodeProcessTrapsSet	User Action	Event	No	Informational	Node $NodeDisplayName ProcessTraps flag is set to $ProcessTraps by $User.	NodeProcessTrapsSet	Common

Description:

The NodeProcessTrapsSet UserAction event provides information when a Node's ProcessTraps flag is set by a user. The ProcessTraps flag indicates to MWTM whether or not to process traps received from the the Node. The value of the ProcessTraps flag indicates the new value.
Possible values of ProcessTraps include:

- True - Traps from the node are to be processed normally.
- False - Traps from the node are to be discarded.

Default Message:

Node $NodeDisplayName ProcessTraps flag is set to $ProcessTraps by $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
NodeState	The current state of the Node.
ProcessTraps	The current state of the ProcessTraps flag.
User	The user who requested the ProcessTraps flag to be set.

Operational Information:

- The setting of the ProcessTraps flag to False can lead to delays in MWTM determining network problems. Caution should be exercised when selecting this value.
  To find the nodes which are currently have the ProcessTraps flag set to false select Node
  folder in the MWTM Main window and sort on the ProcessTraps field.

Go Top

SECTION 4.106

UserAction: ObjectModelPurged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

ObjectModelPurged	User Action	Event	No	Informational	Nodes purged by $User.	ObjectModelPurged	Common

Description:

The ObjectModelPurged UserAction event provides information when an MWTM operator requests during discovery that the MWTM object model database be purged.

Default Message:

Nodes, Linksets, and Links purged by $User.

Message Substitution Variables:

User	The user who requested the MWTM object model database be purged.

Operational Information:

The MWTM object model database can be purged safely as all the data can be rediscovered from the network.

Go Top

SECTION 4.107

UserAction: NodeUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NodeUserDataUpdated	User Action	Event	No	Informational	Node $NodeDisplayName edited by user $User.	NodeUserDataUpdated	Common

Description:

The NodeUserDataUpdated UserAction event provides information when a Node object's user data has been updated by an MWTM user.

Default Message:

Node $NodeDisplayName edited by user $User.

Message Substitution Variables:

Node Substitution variables for Node related data.	
User	The user who requested the Node's data be updated.

Operational Information:

The fields that can be updated for a node include:

- The Node's display name used for identifying the node.
- The Node's icon used for identifying the node type on the MWTM Topology window.
- The Node's SNMPable interfaces used in polling the Node.
- The Node's notes data used for communicating installation dependent information about a Node.

Go Top

SECTION 4.108

UserAction: RtrInterfaceUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RtrInterfaceUserDataUpdated	User Action	Event	No	Informational	Interface $NodeDisplayName/$RtrInterfaceDisplayName edited by user $User.	RtrInterfaceUserDataUpdated	Common

Description:

The RtrInterfaceUserDataUpdated UserAction event provides information when a RtrInterface object's user data has been updated by a MWTM user.

Default Message:

RtrInterface $NodeDisplayName/$RtrInterfaceDisplayName edited by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

RtrInterfaceDisplayName	The name of the RtrInterface.
User	The user who requested the RtrInterface's data be updated.

Operational Information:

The fields that can be updated for a RtrInterface include:

- The RtrInterface's notes data used for communicating installation dependent information about a RtrInterface.

Go Top

SECTION 4.109

UserAction: NodeManagementUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NodeManagementUpdated	User Action	Event	No	Informational	Node $NodeDisplayName has been $ManagementState by user $User.	NodeManagementUpdated	Common

Description:

The NodeManagementUpdated UserAction event provides information when a Node object's management state has been updated by an MWTM user. The value of ManagementState indicates the type of modification. Possible values of ManagementState include:

- Managed - The Node has been marked for management and a discovery poll has been scheduled.
- Unmanaged - The Node is to be unmanaged. All objects owned by this node that are no longer referenced will be removed from MWTM.

Default Message:

Node $NodeDisplayName has been $ManagementState by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

User	The user who requested the Node's management state be updated.

Operational Information:

none.

Go Top

SECTION 4.110

UserAction: DiscoveryRequested

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiscoveryRequested	User Action	Event	No	Informational	Discovery for $Seed, recursion depth $Recursion, requested by user $User.	DiscoveryRequested	Common

Description:

The DiscoveryRequested UserAction event provides information when a user requests the discovery of a seed node.

Default Message:

Discovery for $Seed, recursion depth $Recursion, requested by user $User.

Message Substitution Variables:

Recursion	The recursion level specified by the user for the discovery. 0 for a non-recursive discovery and 255 for a recursive discovery.
Seed	The identifier for the node to be discovered.
User	The user who requested the discovery.

Operational Information:

The use of a non-recursive discovery followed by a recursive discovery can lead to confusing discovery results. See the MWTM User's Guide for a discussion of discovery scenarios.

Go Top

SECTION 4.111

UserAction: PollRequested

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PollRequested	User Action	Event	No	Informational	Poll for $NodeDisplayName requested by user $User.	PollRequested	Common

Description:

The PollRequested UserAction event provides information when a user requests that a Node be polled immediately.

Default Message:

Poll for $NodeDisplayName requested by user $User.

Message Substitution Variables:

Node Substitution variables for Node related data.	
User	The user who requested the Node be polled.

Operational Information:

The use of an immediate poll for a Node can be used to update MWTM's view of the Node between regularly scheduled polling intervals.

Go Top

SECTION 4.112

UserAction: NodeDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NodeDeleted	User Action	Event	No	Informational	Node $NodeDisplayName deleted by user $User.	NodeDeleted	Common

Description:

The NodeDeleted UserAction event provides information when a Node object's deletion from the MWTM object model database is requested.

Default Message:

Node $NodeDisplayName deleted by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

User	The user who requested the Node's data be deleted.

Operational Information:

- The deletion of a node can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.
- The deletion of a node will also cause all of it's rtrinterfaces to be deleted.

Go Top

SECTION 4.113

UserAction: RtrInterfaceDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RtrInterfaceDeleted	User Action	Event	No	Informational	Interface $NodeDisplayName/$RtrInterfaceDisplayName deleted by user $User.	RtrInterfaceDeleted	Common

Description:

The RtrInterfaceDeleted UserAction event provides information when a RtrInterface object's deletion from the MWTM object model database is requested.

Default Message:

Interface $NodeDisplayName/$RtrInterfaceDisplayName deleted by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

RtrInterfaceDisplayName	The display name of the RtrInterface from the MWTM object database.
User	The user who requested the RtrInterface's data be deleted.

Operational Information:

- The deletion of a RtrInterface can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 4.114

UserAction: FileModification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FileModification	User Action	Event	No	Informational	The file $File was $Action by $User.	FileModification	Common
FileModification	User Action	Event	No	Informational	The file $File was $Action by $User.	FileModification	Common
FileModification	User Action	Event	No	Informational	The file $File was $Action by $User.	FileModification	Common

Description:

The FileModification UserAction event provides information when a file on the MWTM server is modified on behalf of an MWTM client. The value of ModificationType indicates the type of modification. Possible values of ModificationType include:

- Create - A new file has been created.
- OverWrite - A file has been over written.
- Delete - A file has been deleted.

Default Message:

The file $File was $Action by $User.

Message Substitution Variables:

File	The name of the file being modified.
Action	The type of modification taking place. One of 'created', 'overwritten', or 'deleted'.
User	The user who requested the discovery.

Operational Information:

Go Top

SECTION 4.115

UserAction: Login

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Login	User Action	Event	No	Normal	$User login Successful from $Host.	Login	Common
Login	User Action	Event	No	Minor	$User login Failed from $Host.	Login	Common
Login	User Action	Event	No	Minor	$User login from $Host was not allowed because the account is disabled.	Login	Common

Description:

The Login UserAction event provides information when an MWTM client attempts to login to the MWTM server. The value of LoginType indicates the success or failure of the login attempt. Possible values of LoginType include:

- Successful - A successful login has occurred.
- Failed - An unsuccessful login has occurred.
- Disabled - A login has been denied because the userid is disabled.

Default Message:

- $User login $LoginType from $Host.
- $User login from $Host was not allowed because the account is disabled.

Message Substitution Variables:

LoginType	The result of the login attempt. One of 'Successful', 'Failed', or 'Disabled'.
User	The User who attempted login to the MWTM server. If MWTM User-Based access is enabled this will be the userid of the user. If MWTM User-Based access is not enabled this will be the hostname of the client machine.
Host	The hostname of the client machine from which the User attempted login to the MWTM server.

Operational Information:

- If the value of LoginType is Failed you may want to look for multiple occurrences for the User as an indicator of unauthorized access attempts.
- If the value of LoginType is Disabled you may want to look for multiple occurrences for the User as an indicator of unauthorized access attempts.

Go Top

SECTION 4.116

UserAction: Logout

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Logout	User Action	Event	No	Normal	$User logout from $Host.	Logout	Common

Logout	User Action	Event	No	Minor	$User logout from $Host. The connection between client and server was lost.	Logout	Common
Logout	User Action	Event	No	Minor	$User logout from $Host. The session was terminated because $User account was administratively disabled or deleted.	Logout	Common
Logout	User Action	Event	No	Normal	$User logout from $Host. Client logout because a new session was started by the user.	Logout	Common

Description:

The Logout UserAction event provides information when an MWTM client islogged out of the MWTM server. The value of LogoutType indicates the type of logout. Possible values of LogoutType include:

- Normal - A normal client logout has occurred.
- ConnectionLost - A client was logged out because the connection between client and server failed.
- NewSession - A client was logged out because the user started a new client session.
- SessionTerminated - A client was logged out because the user was administratively disabled or deleted.

Default Message:

- $User logout from $Host.
- $User logout from $Host. The connection between client and server was lost.
- $User logout from $Host. Client logout because a new session was started by the user.
- $User logout from $Host. The session was terminated because $User account was administratively disabled or deleted.

Message Substitution Variables:

LogoutType	The result of the login attempt. One of 'Normal', 'ConnectionLost', or 'NewSession'.
User	The User who logged out of the MWTM server.
Host	The hostname of the client machine from which the User logged out of the MWTM server.

Operational Information:

Go Top

SECTION 4.117

UserAction: ProvisionRequest

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

ProvisionRequest	User Action	Event	No	Informational	$NodeDisplayName -- Provision request succeeded. $UserName requested to $Operation a $NEType on $FQDN.	ProvisionRequest	Common
ProvisionRequest	User Action	Event	No	Informational	$NodeDisplayName -- Provision request failed. $UserName requested to $Operation a $NEType on $FQDN. Error message: $ErrorMessage.	ProvisionRequest	Common

Description:

The ProvisionRequest UserAction event provides information when auser requests a provisioning operation.

Default Message:

$NodeDisplayName -- Provision request $ProvisionRequestStatus.
$UserName requested to $Operation a $NEType on $FQDN.

Message Substitution Variables:

Node	Substitution variables for Node related data.
FQDN	The fully qualified name of the parent element of the provisioning request.
RDN	The relative name of the parent element of the provisioning request.
ProvisionRequestStatus	Success or Failed
UserName	The user who requested the provsioning operation.
Operation	The provisioning operation. For example: add, modify, or delete.
NEType	The type of the network element that is the subject of the provisioning request.

Go Top

SECTION 4.118

UserAction: LaunchTerminal

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LaunchTerminal	User Action	Event	No	Normal	$User launched Telnet to $Host.	LaunchTerminal	Common
LaunchTerminal	User Action	Event	No	Normal	$User launched SSH to $Host.	LaunchTerminal	Common

Description:

The LaunchTerminal UserAction event reflects when an MWTM client attempts to connect to a node via a terminal. The value of TerminalType indicates the connection protocol used. Possible values of TerminalType include:

- Telnet - A telnet protocol is used.
- SSH - A secure shell protocol is used.

Default Message:

- $User launched $TerminalType to $Host.

Message Substitution Variables:

TerminalType	This is the connection protocol used - one of 'Telnet' or 'SSH'.
User	This is the user who launched the terminal. If MWTM User-Based access is enabled, this will be the userid of the user. If MWTM User-Based access is not enabled, this will be the hostname of the client machine.
Host	This is the hostname of the node to which the user attempts to connect.

Go Top

SECTION 4.119

UserAction: GroupIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GroupIgnoredSet	User Action	Event	No	Informational	Group $GroupDisplayName ignore flag is set to $IgnoredFlag by $User.	GroupIgnoredSet	Common

Description:

The GroupIgnoredSet UserAction event provides information when a Group'sIgnore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the Group in the aggregation algorithm. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The Group is to be excluded from state aggregation.
- False - The Group is to be included in state aggregation.

Default Message:

Group $GroupDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Group
Substitution variables for Group related data.

GroupState	The current state of the Group.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

None.
Go Top

SECTION 4.120

UserAction: GroupUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GroupUserDataUpdated	User Action	Event	No	Informational	Group $GroupDisplayName edited by user $User.	GroupUserDataUpdated	Common

Description:

The GroupUserDataUpdated UserAction event provides information when a Group object's user data has been updated by an MWTM user.

Default Message:

Group $GroupDisplayName edited by user $User.

Message Substitution Variables:

Group
Substitution variables for Group related data.

User	The user who requested the Group's data be updated.

Operational Information:

The fields that can be updated for a Group include:

- The Group's notes data used for communicating information about a Group.

Go Top

SECTION 4.121

UserAction: GroupDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GroupDeleted	User Action	Event	No	Informational	Group $GroupDisplayName deleted by user $User.	GroupDeleted	Common

Description:

The GroupDeleted UserAction event provides information when a Group object'sdeletion from the SGM object model database is requested.

Default Message:

Group $GroupDisplayName deleted by user $User.

Message Substitution Variables:

Group	
Substitution variables for Group related data.	
User	The user who requested the Group's data be deleted.

Operational Information:

None.
Go Top

SECTION 5.1

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigModified	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was modified.	APN-ConfigModified	GGSN

Description:

```
A notification of this type is generated when an              entry is generated in the
cgprsAccPtCfgNotifHistTable and
cgprsAccPtCfgNotifEnable is set to true.
```

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	`This object specifies the access point which has been created, changed or modified.`
cgprsAccPtCfgNotifReason	`This object describes the reason of the notification.`

Go Top

SECTION 5.2

Trap: cgprsAccPtSecSrcViolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-UpstreamSecurityViolation	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- Upstream security violation.	APN-UpstreamSecurityViolation	GGSN

Description:

```
A notification of this type is generated when security                violation as specified by
cgprsAccPtVerifyUpStrTpduSrcAddr occurs on an APN.
```

Default Message:

$NodeDisplayName -- APN ($cgprsAccPtCfgNotifAccPtIndex) Upstream security violation.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtMsAddrType	This object specifies the type of Internet address denoted by cgprsAccPtMsAllocAddr, cgprsAccPtMsNewAddr and cgprsAccPtMsTpduDstAddr.
cgprsAccPtMsAllocAddr	This object specifies the IP address that is assigned to the MS during PDP activation.
cgprsAccPtMsNewAddr	This object specifies the fake IP address that is used by the MS.

Go Top

SECTION 5.3

Trap: cgprsAccPtSecDestViolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-DownstreamSecurityViolation	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- Downstream security violation.	APN-DownstreamSecurityViolation	GGSN

Description:

```
A notification of this type is generated when security                violation as specified by
cgprsAccPtVerifyUpStrTpduDstAddr occurs on an APN.
```

Default Message:

$NodeDisplayName -- APN ($cgprsAccPtCfgNotifAccPtIndex) Downstream security violation.

Message Substitution Variables:

Common	Substitution variables common to all traps.

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtMsAddrType	This object specifies the type of Internet address denoted by cgprsAccPtMsAllocAddr, cgprsAccPtMsNewAddr and cgprsAccPtMsTpduDstAddr.
cgprsAccPtMsAllocAddr	This object specifies the IP address that is assigned to the MS during PDP activation.
cgprsAccPtMsTpduDstAddr	This object specifies the upstream TPDU destination address used by a MS that falls in the reserved range of IP addresses for PLMN devices.

Go Top

SECTION 5.4

Trap: cgprsAccPtMaintenanceNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ServiceMode	Trap	Alarm	Yes	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in maintenance mode.	APN-ServiceMode	GGSN
APN-ServiceMode	Trap	Alarm	Yes	Normal	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in service.	APN-ServiceMode	GGSN
APN-ServiceMode	Poll	Alarm	Yes	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in maintenance mode.	APN-ServiceMode	GGSN
APN-ServiceMode	Poll	Alarm	Yes	Normal	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in service.	APN-ServiceMode	GGSN

Description:

A notification of this type is generated when APN is placed in maintenance mode which is specified by cgprsAccPtOperationMode.

Default Message:

$NodeDisplayName -- The APN ($cgprsAccPtCfgNotifAccPtIndex) is in maintenance mode.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.

Go Top

SECTION 5.5

Trap: cgprsCgInServiceModeNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	GGSN
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	GGSN
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	GGSN
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	GGSN

ChargingGatewayMaintenanceMode	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	GGSN
ChargingGatewayMaintenanceMode	Poll	Alarm	Yes	Warning	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	GGSN

Description:

```
A notification of this type is generated when the         gateway charging function is in normal mode. This can
be identified by cgprsCgServiceMode object.
```

Default Message:

$NodeDisplayName -- The charging gateway is in service.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 5.6

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is down.	ChargingGatewayState	GGSN
ChargingGatewayState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is up.	ChargingGatewayState	GGSN
ChargingGatewayState	Trap	Alarm	Yes	Critical	$NodeDisplayName - The Charging gateway is down	ChargingGatewayState	GGSN
ChargingGatewayState	Trap	Alarm	Yes	Normal	$NodeDisplayName - The Charging gateway is up	ChargingGatewayState	GGSN

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related         alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.

cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 5.7

Trap: cgprsCgGatewaySwitchoverNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewaySwitchover	Trap	Alarm	No	Major	$NodeDisplayName -- The charging gateway switched from $cgprsCgOldChgGatewayAddress to $cgprsCgActiveChgGatewayAddress	ChargingGatewaySwitchover	GGSN
ChargingGatewaySwitchover	Trap	Alarm	No	Major	$NodeDisplayName -- The charging gateway switched from $cgprsCgGatewayGroupStatusOldCgAddr to $cgprsCgGatewayGroupStatusActiveCgAddr	ChargingGatewaySwitchover	GGSN

Description:

A notification of this type is generated when the charging gateway is switched, the new charging gateway is identified by cgprsCgActiveChgGatewayAddress and the old charging gateway is identified by cgprsCgOldChgGatewayAddress.
The switchover will happen according to the value set in cgprsCgGroupSwitchOverTime and the selection of the new CG will be according to the value set in cgprsCgSwitchOverPriority.

Default Message:

$NodeDisplayName -- The charging gateway switched from $cgprsCgOldChgGatewayAddress to $cgprsCgActiveChgGatewayAddress

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgActiveChgGatewayAddrType	This object specifies the address type of the active charging gateway.
cgprsCgActiveChgGatewayAddress	This object specifies the address of the active charging gateway. The type of address will be represented by cgprsCgActiveChgGatewayAddrType.
cgprsCgOldChgGatewayAddress	This object specifies the address of the previous active charging gateway. The type of address will same as the one present in cgprsCgActiveChgGatewayAddrType.

Go Top

SECTION 5.8

Trap: cGtpPathFailedNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPPathFailed	Trap	Alarm	No	Major	$NodeDisplayName -- Peer ($cGtpLastNoRespToEchoGSNIpAddr) failed to respond to the GTP Echo Request.	GTPPathFailed	GGSN

Description:

```
This notification is sent when one of this GSN's peers           failed to respond to the GTP 'Echo Request' message for
the waiting interval.
```

Default Message:

$NodeDisplayName -- Peer ($cGtpLastNoRespToEchoGSNIpAddr) failed to respond to the GTP Echo Request.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGtpLastNoRespToEchoGSNIpAddrTyp	This object indicates the type of Internet address by which cGtpLastNoRespToEchoGSNIpAddr is reachable.
cGtpLastNoRespToEchoGSNIpAddr	The IP address of the last peer GSN device that did not reply to an GTP 'Echo Request' message from the local GSN device.

Go Top

SECTION 5.9

Trap: cGgsnSADccaRatingFailed

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCARatingFail	Trap	Alarm	No	Major	$NodeDisplayName -- The Credit Control Server cannot rate a service request for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCARatingFail	GGSN

Description:

```
This notification is generated when the credit-control          server cannot rate the service request, due to insufficient
rating input, incorrect AVP combination or due to an AVP or
an AVP value that is not recognized or supported in the
rating.
```

Default Message:

$NodeDisplayName -- The Credit Control Server cannot rate a service request for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.

cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 5.10

Trap: cGgsnSADccaEndUsrServDeniedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCAServiceDenied	Trap	Alarm	No	Major	$NodeDisplayName -- The Credit Control Server denied a service request due to service restrictions for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCAServiceDenied	GGSN

Description:

This notification is generated when the credit-control server denies the service request due to service restrictions. On reception of this notif on category level, the CLCI-C shall discard all future user traffic for that category on that PDP context and not attempt to ask for more quotas during the same PDP context.

Default Message:

$NodeDisplayName -- The Credit Control Server denied a service request due to service restrictions for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 5.11

Trap: cGgsnSACsgStateDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CSGState	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The CSG is down.	CSGState	GGSN
CSGState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The CSG is up.	CSGState	GGSN

Description:

This notification is generated when CSG state goes down.

Default Message:

$NodeDisplayName -- The CSG is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnSANotifCsgRealAddressType	This object indicates the type of IP address, for real address of the CSG group.
cGgsnSANotifCsgRealAddress	This object indicates the real IP address of the CSG group.
cGgsnSANotifCsgVirtualAddrType	This object indicates the type of IP address, for virtual address of the CSG group.
cGgsnSANotifCsgVirtualAddress	This object indicates the virtual IP address of the CSG group.
cGgsnSANotifCsgPort	This object indicates the port number of the CSG group.

Go Top

SECTION 5.12

Trap: cGgsnSADccaCreditLimReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCACreditLimitReached	Trap	Alarm	No	Major	$NodeDisplayName -- Credit limit reached for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCACreditLimitReached	GGSN

Description:

This notification is generated when the credit limit is reached. The credit-control server denies the service request since the end user's account could not cover the requested service. Client shall behave exactly as with cGgsnSADccaEndUsrServDeniedNotif.

Default Message:

$NodeDisplayName -- Credit limit reached for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 5.13

Trap: cGgsnSADccaUserUnknownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCAUserUnknown	Trap	Alarm	No	Major	$NodeDisplayName -- User is unknown in the Credit Control Server $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCAUserUnknown	GGSN

Description:

```
This notification is generated when the specified          end user is unknown in the credit-control server.
Such permanent failures cause the client to enter
the Idle state.  The client shall reject or terminate the
PDP context depending on whether the result code was
received in a CCA (Initial) or CCA (Update).
```

Default Message:

$NodeDisplayName -- User is unknown in the Credit Control Server $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 5.14

Trap: cGgsnSADccaAuthRejectedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCAAuthReject	Trap	Alarm	No	Major	$NodeDisplayName -- The Credit Control Server rejected authorization of user $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn.	DCCAAuthReject	GGSN

Description:

```
This notification is generated when credit-control          server failed in authorization of end user.  The PDP
context is deleted and category is blacklisted.
```

Default Message:

$NodeDisplayName -- The Credit Control Server rejected authorization of user $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn.

Message Substitution Variables:

Common	Substitution variables common to all traps.

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 5.15

Trap: cGgsnGlobalErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWServiceState	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The gateway service is shutdown. Reason: $cGgsnHistNotifInfo	GWServiceState	GGSN
GWServiceState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway service is started. Reason: $cGgsnHistNotifInfo	GWServiceState	GGSN

Description:

This notification indicates the occurrence of a gateway related alarm.

Default Message:

$NodeDisplayName -- The gateway service is shutdown.
$NodeDisplayName -- The gateway service is started.
$NodeDisplayName -- MAP-SGSN service is shutdown.
$NodeDisplayName -- MAP-SGSN service is started.
$NodeDisplayName -- No DHCP server is configured.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnGlobalErrorTypes	This object indicates the types of global errors as follows. 'ggsnServiceUp' - Gateway service has started 'ggsnServiceDown' - Gateway service is shutdown 'mapSgsnUp' - MAP-SGSN service has started 'mapSgsnDown' - MAP-SGSN service is shutdown 'noDHCPServer' -- DHCP server is not configured
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm).

	If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

Go Top

SECTION 5.16

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-NoResources	Trap	Alarm	No	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached. Reason: $cGgsnHistNotifInfo	APN-NoResources	GGSN

Description:

This notification indicates the occurrence of a User related alarm.

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 5.17

Trap: cGgsnMaintenanceNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is in maintenance mode.	GWMaintenanceMode	GGSN
GWMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is in service.	GWMaintenanceMode	GGSN
GWMaintenanceMode	Poll	Alarm	Yes	Major	$NodeDisplayName -- The gateway is in maintenance mode.	GWMaintenanceMode	GGSN
GWMaintenanceMode	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is in service.	GWMaintenanceMode	GGSN

Description:

A notification of this type is generated when the gateway is placed in maintenance mode which is specified by cGgsnServiceModeStatus.

Default Message:

$NodeDisplayName -- The gateway is in maintenance mode.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 5.18

Trap: cGgsnAccessPointNameNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-NoRadius	Trap	Alarm	No	Major	APN $ApnDisplayName on the gateway $NodeDisplayName -- No RADIUS server is configured. $cGgsnHistNotifInfo	APN-NoRadius	GGSN

Description:

This notification indicates the occurrence of a APN related alarm.

Default Message:

$NodeDisplayName -- No RADIUS server is configured. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- IP address allocation failed. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- Access point is not reachable. ($cGgsnNotifAccessPointName)

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnAccessPointErrorTypes	This object indicates the types access point errors as follows. 'noRadius' - RADIUS Server is not configured. 'ipAllocationFail' - Unable to allocate IP address. 'apnUnreachable' - Unable to reach access point.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 5.19

Trap: cGgsnMemThresholdClearedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWMemoryThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway memory threshold is cleared. The gateway memory overload protection mechanism is disengaged.	GWMemoryThreshold	GGSN
GWMemoryThreshold	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The gateway memory threshold is reached. The gateway memory overload protection mechanism is engaged.	GWMemoryThreshold	GGSN

Description:

A notification of this type is generated when the gateway retains the memory and falls below threshold value speficied by cGgsnMemoryThreshold.

Default Message:

$NodeDisplayName -- The gateway memory threshold is cleared. The gateway memory overload protection mechanism is disengaged

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 5.20

Trap: cPsdClientDiskFullNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PSDDiskFull	Trap	Alarm	No	Major	$NodeDisplayName -- The PSD $cPsdClientNotifDSServerAddress disk is full. No more CDRs are being stored on the PSD.	PSDDiskFull	GGSN

Description:

```
A notification of this type is generated when the           PSD server's disk become full.
If the disk of writable PSD server becomes full, the
client shall not be able to write any CDR into the
server. It shall then  behave as a retrieve only PSD
server.
```

Default Message:

$NodeDisplayName -- The PSD disk is full. No more CDRs are being stored on the PSD.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cPsdClientNotifDSServerAddrType	This object indicates the type of Internet address of the Data-Store server.
cPsdClientNotifDSServerAddress	This object specifies the Internet address of the Data-Store server . The type of address of an instance of this object is determined by the value of cPsdClientNotifDSServerAddrType.

Go Top

SECTION 5.21

Trap: cPsdClientDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PSDServerState	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The PSD $cPsdClientNotifDSServerAddress is down.	PSDServerState	GGSN
PSDServerState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The PSD $cPsdClientNotifDSServerAddress is up.	PSDServerState	GGSN

Description:

```
A notification of this type is generated when the           PSD server goes DOWN.
If the PSD client was in write/retrieving state, then
that operation shall be be stopped.
```

Default Message:

$NodeDisplayName -- The PSD is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cPsdClientNotifDSServerAddrType	This object indicates the type of Internet address of the Data-Store server.
cPsdClientNotifDSServerAddress	This object specifies the Internet address of the Data-Store server . The type of address of an instance of this object is determined by the value of cPsdClientNotifDSServerAddrType.

Go Top

SECTION 5.22

Trap: cGgsnAccessPointNameNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-IpAllocationFail	Trap	Alarm	No	Critical	APN $ApnDisplayName on the gateway $NodeDisplayName -- IP address allocation failed. $cGgsnHistNotifInfo	APN-IpAllocationFail	GGSN

Description:

This notification indicates the occurrence of a APN related alarm.

Default Message:

$NodeDisplayName -- No RADIUS server is configured. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- IP address allocation failed. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- Access point is not reachable. ($cGgsnNotifAccessPointName)

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnAccessPointErrorTypes	This object indicates the types access point errors as follows. 'noRadius' - RADIUS Server is not configured. 'ipAllocationFail' - Unable to allocate IP address. 'apnUnreachable' - Unable to reach access point.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than

	just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 5.23

Trap: cGgsnAccessPointNameNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-Unreachable	Trap	Alarm	No	Critical	APN $ApnDisplayName on the gateway $NodeDisplayName -- Access point is not reachable. $cGgsnHistNotifInfo	APN-Unreachable	GGSN

Description:

This notification indicates the occurrence of a APN related alarm.

Default Message:

$NodeDisplayName -- No RADIUS server is configured. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- IP address allocation failed. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- Access point is not reachable. ($cGgsnNotifAccessPointName)

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnAccessPointErrorTypes	This object indicates the types access point errors as follows. 'noRadius' - RADIUS Server is not configured. 'ipAllocationFail' - Unable to allocate IP address. 'apnUnreachable' - Unable to reach access point.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 5.24

Trap: cGgsnGlobalErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MapSgsnState	Trap	Alarm	Yes	Major	$NodeDisplayName -- MAP-SGSN service is shutdown. Reason: $cGgsnHistNotifInfo	MapSgsnState	GGSN
MapSgsnState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- MAP-SGSN service is started. Reason: $cGgsnHistNotifInfo	MapSgsnState	GGSN

Description:

```
This notification indicates the occurrence of a gateway        related alarm.
```

Default Message:

$NodeDisplayName -- The gateway service is shutdown.
$NodeDisplayName -- The gateway service is started.
$NodeDisplayName -- MAP-SGSN service is shutdown.
$NodeDisplayName -- MAP-SGSN service is started.
$NodeDisplayName -- No DHCP server is configured.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnGlobalErrorTypes	`This object indicates the types of global errors as follows. 'ggsnServiceUp' - Gateway service has started 'ggsnServiceDown' - Gateway service is shutdown 'mapSgsnUp' - MAP-SGSN service has started 'mapSgsnDown' - MAP-SGSN service is shutdown 'noDHCPServer' -- DHCP server is not configured`
cGgsnHistNotifSeverity	`This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).`
cGgsnHistNotifTimestamp	`This object indicates the value of sysUpTime when this notification was generated.`
cGgsnHistNotifGgsnIpAddrType	`This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.`
cGgsnHistNotifGgsnIpAddr	`The object indicates the IP address that uniquely identifies the device which generated the notification.`
cGgsnHistNotifInfo	`A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.`

Go Top

SECTION 5.25

Trap: cGgsnGlobalErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NoDHCPServer	Trap	Alarm	No	Major	$NodeDisplayName -- No DHCP server is configured. Reason: $cGgsnHistNotifInfo	NoDHCPServer	GGSN

Description:

```
This notification indicates the occurrence of a gateway        related alarm.
```

Default Message:

$NodeDisplayName -- The gateway service is shutdown.
$NodeDisplayName -- The gateway service is started.
$NodeDisplayName -- MAP-SGSN service is shutdown.
$NodeDisplayName -- MAP-SGSN service is started.
$NodeDisplayName -- No DHCP server is configured.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnGlobalErrorTypes	This object indicates the types of global errors as follows. 'ggsnServiceUp' - Gateway service has started 'ggsnServiceDown' - Gateway service is shutdown 'mapSgsnUp' - MAP-SGSN service has started 'mapSgsnDown' - MAP-SGSN service is shutdown 'noDHCPServer' -- DHCP server is not configured
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

Go Top

SECTION 5.26

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-AuthenticationFail	Trap	Alarm	No	Minor	APN $ApnDisplayName on gateway $NodeDisplayName -- A PDP activation failed because of an authentication failure. Reason: $cGgsnHistNotifInfo	APN-AuthenticationFail	GGSN

Description:

```
This notification indicates the occurrence of a User        related alarm.
```

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 5.27

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-CCRInitFail	Trap	Alarm	No	Minor	APN $ApnDisplayName on gateway $NodeDisplayName -- The TX timer expired before getting a CCR (initial) response. Reason: $cGgsnHistNotifInfo	APN-CCRInitFail	GGSN

Description:

```
This notification indicates the occurrence of a User        related alarm.
```

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 5.28

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-QuotaPushFail	Trap	Alarm	No	Minor	APN $ApnDisplayName on gateway $NodeDisplayName -- Quota Push failed to the CSG quota server. Reason: $cGgsnHistNotifInfo	APN-QuotaPushFail	GGSN

Description:

```
This notification indicates the occurrence of a User        related alarm.
```

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the

	user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 5.29

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigCreated	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was created.	APN-ConfigCreated	GGSN

Description:

A notification of this type is generated when an entry is generated in the cgprsAccPtCfgNotifHistTable and cgprsAccPtCfgNotifEnable is set to true.

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 5.30

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigDeleted	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was deleted.	APN-ConfigDeleted	GGSN

Description:

A notification of this type is generated when an entry is generated in the cgprsAccPtCfgNotifHistTable and cgprsAccPtCfgNotifEnable is set to true.

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 5.31

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingTransferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.	ChargingTransferState	GGSN
ChargingTransferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.	ChargingTransferState	GGSN
ChargingTransferState	Trap	Alarm	Yes	Major	$NodeDisplayName - The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway	ChargingTransferState	GGSN
ChargingTransferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.	ChargingTransferState	GGSN

Description:

A cgprsCgAlarmNotif signifies that a GPRS related alarm is detected in the managed system. This alarm is sent after an entry has been added to cgprsCgAlarmHistTable.

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
	Type of the GPRS charging gateway or charging related

cgprsCgAlarmHistType	alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 5.32

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingCapacityState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.	ChargingCapacityState	GGSN
ChargingCapacityState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.	ChargingCapacityState	GGSN
ChargingCapacityState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.	ChargingCapacityState	GGSN
ChargingCapacityState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs	ChargingCapacityState	GGSN

Description:

A cgprsCgAlarmNotif signifies that a GPRS related alarm is detected in the managed system. This alarm is sent after an entry has been added to cgprsCgAlarmHistTable.

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.

cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 5.33

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayEchoState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.	ChargingGatewayEchoState	GGSN
ChargingGatewayEchoState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway received an echo response from the charging gateway.	ChargingGatewayEchoState	GGSN
ChargingGatewayEchoState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.	ChargingGatewayEchoState	GGSN
ChargingGatewayEchoState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway received an echo response from the charging gateway.	ChargingGatewayEchoState	GGSN

Description:

A cgprsCgAlarmNotif signifies that a GPRS related alarm is detected in the managed system. This alarm is sent after an entry has been added to cgprsCgAlarmHistTable.

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 5.34

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingCDRBufferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has discarded G-CDRs.	ChargingCDRBufferState	GGSN
ChargingCDRBufferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.	ChargingCDRBufferState	GGSN
ChargingCDRBufferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has discarded G-CDRs.	ChargingCDRBufferState	GGSN
ChargingCDRBufferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.	ChargingCDRBufferState	GGSN

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	`Type of the GPRS charging gateway or charging related alarm.`
cgprsCgAlarmHistAddrType	`This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.`
cgprsCgAlarmHistAddress	`The IP address that is used to uniquely identify the CG.`
cgprsCgAlarmHistSeverity	`This object indicates the severity of the alarm.`
cgprsCgAlarmHistInfo	`This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.`

Go Top

SECTION 5.35

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging transactions on the gateway are disabled.	ChargingState	GGSN
ChargingState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging transactions on the gateway are enabled.	ChargingState	GGSN
ChargingState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging transactions on the gateway are disabled.	ChargingState	GGSN
ChargingState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging transactions on the gateway are enabled	ChargingState	GGSN

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 5.36

Trap: ciscoDiaBaseProtPeerConnectionDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPeerConnectionState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	GGSN
DiameterPeerConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	GGSN
DiameterPeerConnectionState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	GGSN

DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	GGSN
DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	GGSN
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitConnAck.	DiameterPeerConnectionState	GGSN
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitICEA.	DiameterPeerConnectionState	GGSN
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is elect.	DiameterPeerConnectionState	GGSN
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitReturns.	DiameterPeerConnectionState	GGSN
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is closing.	DiameterPeerConnectionState	GGSN

Description:

```
An ciscoDiaBaseProtPeerConnectionDownNotif notification           is sent when both the following conditions are true:
1) the value of
ciscoDiaBaseProtEnablePeerConnectionDownNotif is true(1)
2) cdbpPeerStatsState changes to closed(1).
It can be utilized by an NMS to trigger logical/physical
entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The peer $cdbpPeerId state is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpLocalId	The implementation identification string for the Diameter software in use on the system, for example; 'diameterd'
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 5.37

Trap: ciscoDiaBaseProtPermanentFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPermanentFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol permanent failures for the diameter peer $cdbpPeerId has increased.	DiameterPermanentFailure	GGSN

Description:

```
An ciscoDiaBaseProtPermanentFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnablePermanentFailureNotif
   is true(1)
2) the value of cdbpPeerStatsPermanentFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol permanent failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsPermanentFailures	This object represents the Number of permanent failures returned to peer.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 5.38

Trap: ciscoDiaBaseProtProtocolErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterProtocolError	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol errors returned to the diameter peer $cdbpPeerId has increased.	DiameterProtocolError	GGSN

Description:

```
An ciscoDiaBaseProtProtocolErrorNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableProtocolErrorNotif
   is true(1)
2) the value of cdbpPeerStatsProtocolErrors changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol errors returned to the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsProtocolErrors	This object represents the Number of protocol errors returned to peer, but not including redirects.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 5.39

Trap: ciscoDiaBaseProtTransientFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterTransientFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol transient failures for the diameter peer $cdbpPeerId has increased.	DiameterTransientFailure	GGSN

Description:

```
An ciscoDiaBaseProtTransientFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableTransientFailureNotif
   is true(1)
2) the value of cdbpPeerStatsTransientFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol transient failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsTransientFailures	This object represents the transient failure count.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 5.40

Trap: cIscsiInstSessionFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-InstanceSessionState	Trap	Alarm	No	Warning	$NodeDisplayName - The active session has failed for the remote node - $cIscsiInstLastSsnRmtNodeName.	iSCSI-InstanceSessionState	GGSN

Description:

```
Sent when an active session is failed by either the initiator        or the target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The active session has failed for the remote node $cIscsiInstLastSsnRmtNodeName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiInstSsnFailures	This object counts the number of times a session belonging to this instance has been failed.
cIscsiInstLastSsnFailureType	The counter object in the cIscsiInstSsnErrorStatsTable that was incremented when the last session failure occurred. If the reason for failure is not found in the cIscsiInstSsnErrorStatsTable, the value { 0.0 } is used instead.
cIscsiInstLastSsnRmtNodeName	An octet string describing the name of the remote node from the failed session.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular

	ISCSI instance.

Go Top

SECTION 5.41

Trap: cIscsiIntrLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-InitiatorLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.	iSCSI-InitiatorLoginStatus	GGSN

Description:

```
Sent when a login is failed by a initiator.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiIntrLastTgtFailureAddrType	The type of Internet Network Address in cIscsiIntrLastTgtFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated

	if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiIntrLoginFailures	This object counts the number of times a login attempt from this local initiator has failed.
cIscsiIntrLastFailureType	The type of the most recent failure of a login attempt from this initiator, represented as the OID of the counter object in cIscsiInitiatorLoginStatsTable for which the relevant instance was incremented. A value of 0.0 indicates a type which is not represented by any of the counters in cIscsiInitiatorLoginStatsTable.
cIscsiIntrLastTgtFailureName	An octet string giving the name of the target that failed the last login attempt.
cIscsiIntrLastTgtFailureAddr	An Internet Network Address giving the host address of the target that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

SECTION 5.42

Trap: cIscsiTgtLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-TargetLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.	iSCSI-TargetLoginStatus	GGSN

Description:

```
Sent when a login is failed by a target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiTgtLastIntrFailureAddrType	The type of Internet Network Address in cIscsiTgtLastIntrFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the

	InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiTgtLoginFailures	This object counts the number of times a login attempt to this local target has failed.
cIscsiTgtLastFailureType	The type of the most recent failure of a login attempt to this target, represented as the OID of the counter object in cIscsiTargetLoginStatsTable for which the relevant instance was incremented. A value of 0.0 indicates a type which is not represented by any of the counters in cIscsiTargetLoginStatsTable.
cIscsiTgtLastIntrFailureName	An octet string giving the name of the initiator that failed the last login attempt.
cIscsiTgtLastIntrFailureAddr	An Internet Network Address giving the host address of the initiator that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

SECTION 5.43

Trap: cGgsnSACsgR100StateUpNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CSGGroupState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The CSG Group $cGgsnSANotifCsgName: $cGgsnSANotifCsgPort is up.	CSGGroupState	GGSN
CSGGroupState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The CSG Group $cGgsnSANotifCsgName: $cGgsnSANotifCsgPort is down	CSGGroupState	GGSN

Description:

```
This notification is generated when CSG state goes        up. The objects in the varbind list represents -
cGgsnSANotifCsgName: CSG group Name.
cGgsnSANotifCsgRealAddressType: Type of CSG group real
                                IP address.
cGgsnSANotifCsgRealAddress: Real IP address of the
                            CSG group.
cGgsnSANotifCsgVirtualAddrType: Type of CSG group virtual
                                IP address.
cGgsnSANotifCsgVirtualAddress: Virtual IP address of the
                               CSG group.
cGgsnSANotifCsgPort: CSG group port number.
```

Default Message:

$NodeDisplayName -- The CSG Group $ cGgsnSANotifCsgName:$cGgsnSANotifCsgPort is up.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnSANotifCsgRealAddressType	This object indicates the type of IP address, for real address of the CSG group. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cGgsnSANotifCsgVirtualAddrType	This object indicates the type of IP address, for virtual address of the CSG group. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z

	textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cGgsnSANotifCsgName	This object indicates the CSG group name in cGgsnSACsgEntry.
cGgsnSANotifCsgRealAddress	This object indicates the real IP address of the CSG group.
cGgsnSANotifCsgVirtualAddress	This object indicates the virtual IP address of the CSG group.
cGgsnSANotifCsgPort	This object indicates the port number of the CSG group.

Go Top

SECTION 5.44

Trap: ciscoTap2MediationTimedOut

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationTimedOut	Trap	Alarm	Yes	Normal	$NodeDisplayName - Tap2Mediation status is active.	Tap2MediationTimedOut	GGSN
Tap2MediationTimedOut	Trap	Alarm	Yes	Critical	$NodeDisplayName - Tap2Mediation status is notInService.	Tap2MediationTimedOut	GGSN
Tap2MediationTimedOut	Trap	Alarm	Yes	Warning	$NodeDisplayName - Tap2Mediation status is notReady.	Tap2MediationTimedOut	GGSN
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndGo.	Tap2MediationTimedOut	GGSN
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndWait.	Tap2MediationTimedOut	GGSN
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is destroy.	Tap2MediationTimedOut	GGSN

Description:

```
When an intercept is autonomously removed by an intercepting        device, such as due to the time specified in
cTap2MediationTimeout arriving, the device notifies the manager
of the action.
```

Default Message:

$NodeDisplayName - Tap2Mediation status is active.
$NodeDisplayName - Tap2Mediation status is notReady.
$NodeDisplayName - Tap2Mediation status is notInService.
$NodeDisplayName - Tap2Mediation status is createAndGo.
$NodeDisplayName - Tap2Mediation status is createAndWait.
$NodeDisplayName - Tap2Mediation status is destroy.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2MediationStatus	The status of this conceptual row. This object is used to

manage creation, modification and deletion of rows in this table.
cTap2MediationTimeout may be modified at any time (even while the row is active). But when the row is active, the other writable objects may not be modified without setting its value to 'notInService'.
The entry may not be deleted or deactivated by setting its value to 'destroy' or 'notInService' if there is any associated entry in cTap2StreamTable.
The RowStatus textual convention is used to manage the creation and deletion of conceptual rows, and is used as the value of the SYNTAX clause for the status column of a conceptual row (as described in Section 7.7.1 of [2].)
The status column has six defined values:
- `active', which indicates that the conceptual row is available for use by the managed device;
- `notInService', which indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device (see NOTE below);
- `notReady', which indicates that the conceptual row exists in the agent, but is missing information necessary in order to be available for use by the managed device;
- `createAndGo', which is supplied by a management station wishing to create a new instance of a conceptual row and to have its status automatically set to active, making it available for use by the managed device;
- `createAndWait', which is supplied by a management station wishing to create a new instance of a conceptual row (but not make it available for use by the managed device); and,
- `destroy', which is supplied by a management station wishing to delete all of the instances associated with an existing conceptual row.
Whereas five of the six values (all except `notReady') may be specified in a management protocol set operation, only three values will be returned in response to a management protocol retrieval operation: `notReady', `notInService' or `active'. That is, when queried, an existing conceptual row has only three states: it is either available for use by the managed device (the status column has value `active'); it is not available for use by the managed device, though the agent has sufficient information to make it so (the status column has value `notInService'); or, it is not available for use by the managed device, and an attempt to make it so would fail because the agent has insufficient information (the state column has value `notReady').
NOTE WELL
This textual convention may be used for a MIB table, irrespective of whether the values of that table's conceptual rows are able to be modified while it is active, or whether its conceptual rows must be taken out of service in order to be modified. That is, it is the responsibility of the DESCRIPTION clause of the status column to specify whether the status column must not be `active' in order for the value of some other column of the same conceptual row to be modified. If such a specification is made, affected columns may be changed by an SNMP set PDU if the RowStatus would not be equal to `active' either immediately before or after processing the PDU. In other words, if the PDU also contained a varbind that would change the RowStatus value, the column in question may be changed if the RowStatus was not equal to `active' as the PDU was received, or if the varbind sets the status to a value other than 'active'.
Also note that whenever any elements of a row exist, the RowStatus column must also exist.
To summarize the effect of having a conceptual row with a status column having a SYNTAX clause value of RowStatus,

consider the following state diagram:

STATE

| A | B | C | D

| |status col.|status column|

|status column | is | is |status column

ACTION |does not exist| notReady | notInServiceis active

set status |noError ->D|inconsist- |inconsistent-|inconsistent-

column to | or | entValue| Value| Value

createAndGo |inconsistent- | | |

| Value| | |

set status |noError see 1|inconsist- |inconsistent-|inconsistent-

column to | or | entValue| Value| Value

createAndWait |wrongValue | | |

set status |inconsistent- |inconsist- |noError |noError

column to | Value| entValue| |

active | | | |

| | or | |

| | | |

| |see 2 ->D| ->D| ->D

set status |inconsistent- |inconsist- |noError |noError ->C

column to | Value| entValue| |

notInService | | | |

| | or | | or

| | | |

| |see 3 ->C| ->C|wrongValue

set status |noError |noError |noError |noError

column to | | | |

destroy | ->A| ->A| ->A| ->A

set any other |see 4 |noError |noError |see 5

column to some| | | |

value | | see 1| ->C| ->D

(1) goto B or C, depending on information available to the agent.

(2) if other variable bindings included in the same PDU, provide values for all columns which are missing but required, then return noError and goto D.

(3) if other variable bindings included in the same PDU, provide values for all columns which are missing but required, then return noError and goto C.

(4) at the discretion of the agent, the return value may be either:

inconsistentName: because the agent does not choose to create such an instance when the corresponding RowStatus instance does not exist, or

inconsistentValue: if the supplied value is inconsistent with the state of some other MIB object's value, or

noError: because the agent chooses to create the instance.

If noError is returned, then the instance of the status column must also be created, and the new state is B or C, depending on the information available to the agent. If inconsistentName or inconsistentValue is returned, the row remains in state A.

(5) depending on the MIB definition for the column/table, either noError or inconsistentValue may be returned.

NOTE: Other processing of the set request may result in a response other than noError being returned, e.g., wrongValue, noCreation, etc.

Conceptual Row Creation

There are four potential interactions when creating a conceptual row: selecting an instance-identifier which is not in use; creating the conceptual row; initializing any

objects for which the agent does not supply a default; and,
making the conceptual row available for use by the managed
device.
Interaction 1: Selecting an Instance-Identifier
The algorithm used to select an instance-identifier varies
for each conceptual row. In some cases, the instance-
identifier is semantically significant, e.g., the
destination address of a route, and a management station
selects the instance-identifier according to the semantics.
In other cases, the instance-identifier is used solely to
distinguish conceptual rows, and a management station
without specific knowledge of the conceptual row might
examine the instances present in order to determine an
unused instance-identifier. (This approach may be used, but
it is often highly sub-optimal; however, it is also a
questionable practice for a naive management station to
attempt conceptual row creation.)
Alternately, the MIB module which defines the conceptual row
might provide one or more objects which provide assistance
in determining an unused instance-identifier. For example,
if the conceptual row is indexed by an integer-value, then
an object having an integer-valued SYNTAX clause might be
defined for such a purpose, allowing a management station to
issue a management protocol retrieval operation. In order
to avoid unnecessary collisions between competing management
stations, `adjacent' retrievals of this object should be
different.
Finally, the management station could select a pseudo-random
number to use as the index. In the event that this index
was already in use and an inconsistentValue was returned in
response to the management protocol set operation, the
management station should simply select a new pseudo-random
number and retry the operation.
A MIB designer should choose between the two latter
algorithms based on the size of the table (and therefore the
efficiency of each algorithm). For tables in which a large
number of entries are expected, it is recommended that a MIB
object be defined that returns an acceptable index for
creation. For tables with small numbers of entries, it is
recommended that the latter pseudo-random index mechanism be
used.
Interaction 2: Creating the Conceptual Row
Once an unused instance-identifier has been selected, the
management station determines if it wishes to create and
activate the conceptual row in one transaction or in a
negotiated set of interactions.
Interaction 2a: Creating and Activating the Conceptual Row
The management station must first determine the column
requirements, i.e., it must determine those columns for
which it must or must not provide values. Depending on the
complexity of the table and the management station's
knowledge of the agent's capabilities, this determination
can be made locally by the management station. Alternately,
the management station issues a management protocol get
operation to examine all columns in the conceptual row that
it wishes to create. In response, for each column, there
are three possible outcomes:
- a value is returned, indicating that some other
management station has already created this conceptual
row. We return to interaction 1.
- the exception `noSuchInstance' is returned,
indicating that the agent implements the object-type
associated with this column, and that this column in at
least one conceptual row would be accessible in the MIB
view used by the retrieval were it to exist. For those
columns to which the agent provides read-create access,
the `noSuchInstance' exception tells the management
station that it should supply a value for this column
when the conceptual row is to be created.
- the exception `noSuchObject' is returned, indicating
that the agent does not implement the object-type

associated with this column or that there is no conceptual row for which this column would be accessible in the MIB view used by the retrieval. As such, the management station can not issue any management protocol set operations to create an instance of this column.

Once the column requirements have been determined, a management protocol set operation is accordingly issued. This operation also sets the new instance of the status column to `createAndGo'.

When the agent processes the set operation, it verifies that it has sufficient information to make the conceptual row available for use by the managed device. The information available to the agent is provided by two sources: the management protocol set operation which creates the conceptual row, and, implementation-specific defaults supplied by the agent (note that an agent must provide implementation-specific defaults for at least those objects which it implements as read-only). If there is sufficient information available, then the conceptual row is created, a `noError' response is returned, the status column is set to `active', and no further interactions are necessary (i.e., interactions 3 and 4 are skipped). If there is insufficient information, then the conceptual row is not created, and the set operation fails with an error of `inconsistentValue'. On this error, the management station can issue a management protocol retrieval operation to determine if this was because it failed to specify a value for a required column, or, because the selected instance of the status column already existed. In the latter case, we return to interaction 1. In the former case, the management station can re-issue the set operation with the additional information, or begin interaction 2 again using `createAndWait' in order to negotiate creation of the conceptual row.

NOTE WELL

Regardless of the method used to determine the column requirements, it is possible that the management station might deem a column necessary when, in fact, the agent will not allow that particular columnar instance to be created or written. In this case, the management protocol set operation will fail with an error such as `noCreation' or `notWritable'. In this case, the management station decides whether it needs to be able to set a value for that particular columnar instance. If not, the management station re-issues the management protocol set operation, but without setting a value for that particular columnar instance; otherwise, the management station aborts the row creation algorithm.

Interaction 2b: Negotiating the Creation of the Conceptual Row

The management station issues a management protocol set operation which sets the desired instance of the status column to `createAndWait'. If the agent is unwilling to process a request of this sort, the set operation fails with an error of `wrongValue'. (As a consequence, such an agent must be prepared to accept a single management protocol set operation, i.e., interaction 2a above, containing all of the columns indicated by its column requirements.) Otherwise, the conceptual row is created, a `noError' response is returned, and the status column is immediately set to either `notInService' or `notReady', depending on whether it has sufficient information to make the conceptual row available for use by the managed device. If there is sufficient information available, then the status column is set to `notInService'; otherwise, if there is insufficient information, then the status column is set to `notReady'. Regardless, we proceed to interaction 3.

Interaction 3: Initializing non-defaulted Objects

The management station must now determine the column

requirements. It issues a management protocol get operation to examine all columns in the created conceptual row. In the response, for each column, there are three possible outcomes:
- a value is returned, indicating that the agent implements the object-type associated with this column and had sufficient information to provide a value. For those columns to which the agent provides read-create access (and for which the agent allows their values to be changed after their creation), a value return tells the management station that it may issue additional management protocol set operations, if it desires, in order to change the value associated with this column.
- the exception `noSuchInstance' is returned, indicating that the agent implements the object-type associated with this column, and that this column in at least one conceptual row would be accessible in the MIB view used by the retrieval were it to exist. However, the agent does not have sufficient information to provide a value, and until a value is provided, the conceptual row may not be made available for use by the managed device. For those columns to which the agent provides read-create access, the `noSuchInstance' exception tells the management station that it must issue additional management protocol set operations, in order to provide a value associated with this column.
- the exception `noSuchObject' is returned, indicating that the agent does not implement the object-type associated with this column or that there is no conceptual row for which this column would be accessible in the MIB view used by the retrieval. As such, the management station can not issue any management protocol set operations to create an instance of this column.

If the value associated with the status column is `notReady', then the management station must first deal with all `noSuchInstance' columns, if any. Having done so, the value of the status column becomes `notInService', and we proceed to interaction 4.

Interaction 4: Making the Conceptual Row Available

Once the management station is satisfied with the values associated with the columns of the conceptual row, it issues a management protocol set operation to set the status column to `active'. If the agent has sufficient information to make the conceptual row available for use by the managed device, the management protocol set operation succeeds (a `noError' response is returned). Otherwise, the management protocol set operation fails with an error of `inconsistentValue'.

NOTE WELL

A conceptual row having a status column with value `notInService' or `notReady' is unavailable to the managed device. As such, it is possible for the managed device to create its own instances during the time between the management protocol set operation which sets the status column to `createAndWait' and the management protocol set operation which sets the status column to `active'. In this case, when the management protocol set operation is issued to set the status column to `active', the values held in the agent supersede those used by the managed device.

If the management station is prevented from setting the status column to `active' (e.g., due to management station or network failure) the conceptual row will be left in the `notInService' or `notReady' state, consuming resources indefinitely. The agent must detect conceptual rows that have been in either state for an abnormally long period of time and remove them. It is the responsibility of the DESCRIPTION clause of the status column to indicate what an abnormally long period of time would be. This period of time should be long enough to allow for human response time

	(including `think time') between the creation of the conceptual row and the setting of the status to `active'. In the absense of such information in the DESCRIPTION clause, it is suggested that this period be approximately 5 minutes in length. This removal action applies not only to newly-created rows, but also to previously active rows which are set to, and left in, the notInService state for a prolonged period exceeding that which is considered normal for such a conceptual row. Conceptual Row Suspension When a conceptual row is `active', the management station may issue a management protocol set operation which sets the instance of the status column to `notInService'. If the agent is unwilling to do so, the set operation fails with an error of `wrongValue'. Otherwise, the conceptual row is taken out of service, and a `noError' response is returned. It is the responsibility of the DESCRIPTION clause of the status column to indicate under what circumstances the status column should be taken out of service (e.g., in order for the value of some other column of the same conceptual row to be modified). Conceptual Row Deletion For deletion of conceptual rows, a management protocol set operation is issued which sets the instance of the status column to `destroy'. This request may be made regardless of the current value of the status column (e.g., it is possible to delete conceptual rows which are either `notReady', `notInService' or `active'.) If the operation succeeds, then all instances associated with the conceptual row are immediately removed.
cTap2MediationContentId	cTap2MediationContentId is a session identifier, from the intercept application's perspective, and a content identifier from the Mediation Device's perspective. The Mediation Device is responsible for making sure these are unique, although the SNMP RowStatus row creation process will help by not allowing it to create conflicting entries. Before creating a new entry, a value for this variable may be obtained by reading cTap2MediationNewIndex to reduce the probability of a value collision.

Go Top

SECTION 5.45

Trap: ciscoNtpGeneralConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with all NTP servers is lost	NtpConnectionState	GGSN
NtpConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with NTP server has been restored	NtpConnectionState	GGSN

Description:

```
This trap is sent when the device loses connectivity            to all NTP servers.
```

Default Message:

$NodeDisplayName - Connection with all NTP servers is lost.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 5.46

Trap: ciscoNtpHighPriorityConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with the high priority NTP server is failed	NtpHighPriorityConnectionState	GGSN
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with the high priority NTP server is restored	NtpHighPriorityConnectionState	GGSN

Description:

```
A failure to connect with an high priority NTP server           (e.g. a server at the lowest stratum) is detected.
```

Default Message:

$NodeDisplayName - Connection with the high priority NTP server is failed

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpPeersPeerAddress	The IP address of the peer. When creating a new association, a value should be set either for this object or the corresponding instance of cntpPeersPeerName, before the row is made active.
cntpPeersAssocId	An integer value greater than 0 that uniquely identifies a peer with which the local NTP server is associated.

Go Top

SECTION 5.47

Trap: ciscoNtpSrvStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpServerStatus	Trap	Alarm	Yes	Indeterminate	$NodeDisplayName - The NTP server status is unknown	NtpServerStatus	GGSN
NtpServerStatus	Trap	Alarm	Yes	Critical	$NodeDisplayName - The NTP server is not running	NtpServerStatus	GGSN
NtpServerStatus	Trap	Alarm	Yes	Warning	$NodeDisplayName - The NTP server is not synchronized to any time source	NtpServerStatus	GGSN
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to its own local clock	NtpServerStatus	GGSN
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a local hardware refclock	NtpServerStatus	GGSN
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a remote NTP server	NtpServerStatus	GGSN

Description:

```
This notification is generated whenever the value of           cntpSysSrvStatus changes.
```

Default Message:

$NodeDisplayName - The NTP server status is unknown
$NodeDisplayName - The NTP server is not running
$NodeDisplayName - The NTP server is not synchronized to any time source
$NodeDisplayName - The NTP server is synchronized to its own local clock

$NodeDisplayName - The NTP server is synchronized to a local hardware refclock
$NodeDisplayName - The NTP server is synchronized to a remote NTP server

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpSysSrvStatus	Current state of the NTP server with values coded as follows: 1: server status is unknown 2: server is not running 3: server is not synchronized to any time source 4: server is synchronized to its own local clock 5: server is synchronized to a local hardware refclock (e.g. GPS) 6: server is synchronized to a remote NTP server INTEGER is unknown

Go Top

SECTION 5.48

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is above the high threshold of $GGSNHighThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	GGSN
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	GGSN
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is below the low threshold of $GGSNLowThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the

Roman";">GPDUBytesSentRateThreshold	rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the

Roman";">IPOutboundDiscardsThreshold	number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.49

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is above the high threshold of $GGSNHighThreshold percent of total signalling messages received.	GTPUnexpectedMsgsThreshold	GGSN
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total signalling messages received.	GTPUnexpectedMsgsThreshold	GGSN

GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is below the low threshold of $GGSNLowThreshold percent of the total signalling messages received.	GTPUnexpectedMsgsThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low

	threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.50

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is above the high threshold of $GGSNHighThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	GGSN
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	GGSN
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is below the low threshold of $GGSNLowThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	Alarm Description
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the

Roman";">IPOutboundNoRoutesThreshold	number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.51

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is above the high threshold of $GGSNHighThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	GGSN
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	GGSN
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is below the low threshold of $GGSNLowThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	Alarm Description
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.52

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is above the high threshold of $GGSNHighThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	GGSN
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	GGSN
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is below the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes

	received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.

width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.53

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is above the high threshold of $GGSNHighThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	GGSN
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	GGSN
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is below the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**

width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.

width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.54

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ActiveGTPVersion0PDPsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of active GTP version 0 PDP contexts is $GGSNThresholdValue percent of the active GTP version 0 PDP contexts limit which is above the high threshold of $GGSNHighThreshold percent of the active GTP version 0 PDP contexts limit.	ActiveGTPVersion0PDPsThreshold	GGSN
ActiveGTPVersion0PDPsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of active GTP version 0 PDP contexts is $GGSNThresholdValue percent of the active GTP version 0 PDP contexts limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the active GTP version 0 PDP contexts limit.	ActiveGTPVersion0PDPsThreshold	GGSN
ActiveGTPVersion0PDPsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of active GTP version 0 PDP contexts is $GGSNThresholdValue percent of the active GTP version 0 PDP contexts limit which is below the low threshold of $GGSNLowThreshold percent of the active GTP version 0 PDP contexts limit.	ActiveGTPVersion0PDPsThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family:	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the

Roman";">IPReassemblyFailuresThreshold	number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.55

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ActiveGTPVersion1PDPsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of active GTP version 1 PDP contexts is $GGSNThresholdValue percent of the active GTP version 1 PDP contexts limit which is above the high threshold of $GGSNHighThreshold percent of the active GTP version 1 PDP contexts limit.	ActiveGTPVersion1PDPsThreshold	GGSN
ActiveGTPVersion1PDPsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of active GTP version 1 PDP contexts is $GGSNThresholdValue percent of the active GTP version 1 PDP contexts limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the active GTP version 1 PDP contexts limit.	ActiveGTPVersion1PDPsThreshold	GGSN
ActiveGTPVersion1PDPsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of active GTP version 1 PDP contexts is $GGSNThresholdValue percent of the active GTP version 1 PDP contexts limit which is below the low threshold of $GGSNLowThreshold percent of the active GTP version 1 PDP contexts limit.	ActiveGTPVersion1PDPsThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289">	width="516">

style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.56

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is above the high threshold of $GGSNHighThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	GGSN
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	GGSN
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is below the low threshold of $GGSNLowThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the

Roman";">RejectedPDPContextsThreshold	number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the

	number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.57

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPInboundHeaderErrorsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of inbound datagrams with header errors is $GGSNThresholdValue percent of total inbound datagrams which is above the high threshold of $GGSNHighThreshold percent of total inbound datagrams.	IPInboundHeaderErrorsThreshold	GGSN
IPInboundHeaderErrorsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of inbound datagrams with header errors is $GGSNThresholdValue percent of total inbound datagrams which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total inbound datagrams.	IPInboundHeaderErrorsThreshold	GGSN
IPInboundHeaderErrorsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of inbound datagrams with header errors is $GGSNThresholdValue percent of total inbound datagrams which is below the low threshold of $GGSNLowThreshold percent of total inbound datagrams.	IPInboundHeaderErrorsThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.

width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.

width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPOutboundNoRoutesThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of outbound datagrams discarded because of no route is $GGSNThresholdValue percent of outbound datagram requests which is above the high threshold of $GGSNHighThreshold percent of outbound datagram requests.	IPOutboundNoRoutesThreshold	GGSN
IPOutboundNoRoutesThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of outbound datagrams discarded because of no route is $GGSNThresholdValue percent of outbound datagram requests which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of outbound datagram requests.	IPOutboundNoRoutesThreshold	GGSN
IPOutboundNoRoutesThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of outbound datagrams discarded because of no route is $GGSNThresholdValue percent of outbound datagram requests which is below the low threshold of $GGSNLowThreshold percent of outbound datagram requests.	IPOutboundNoRoutesThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the

Roman";">UDPIncomingErrorsThreshold	number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.59

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPReassemblyFailuresThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of IP reassembly failures is $GGSNThresholdValue percent of inbound datagrams which is above the high threshold of $GGSNHighThreshold percent of inbound datagrams.	IPReassemblyFailuresThreshold	GGSN
IPReassemblyFailuresThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of IP reassembly failures is $GGSNThresholdValue percent of inbound datagrams which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of inbound datagrams.	IPReassemblyFailuresThreshold	GGSN
IPReassemblyFailuresThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of IP reassembly failures is $GGSNThresholdValue percent of inbound datagrams which is below the low threshold of $GGSNLowThreshold percent of inbound datagrams.	IPReassemblyFailuresThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of

	total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total

	inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.60

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
					$NodeDisplayName - The number of UDP datagrams received in error is		

UDPIncomingErrorsThreshold	Poll	Alarm	Yes	Major	$GGSNThresholdValue percent of the number of UDP datagrams delivered which is above the high threshold of $GGSNHighThreshold percent of the number of UDP datagrams delivered.	UDPIncomingErrorsThreshold	GGSN
UDPIncomingErrorsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of UDP datagrams received in error is $GGSNThresholdValue percent of the number of UDP datagrams delivered which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the number of UDP datagrams delivered.	UDPIncomingErrorsThreshold	GGSN
UDPIncomingErrorsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of UDP datagrams received in error is $GGSNThresholdValue percent of the number of UDP datagrams delivered which is below the low threshold of $GGSNLowThreshold percent of the number of UDP datagrams delivered.	UDPIncomingErrorsThreshold	GGSN

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the

	number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.

width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 5.61

Trap: cGgsnPdfStateDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PdfStateDown	Trap	Event	No	Warning	The cGgsnPdfStateDownNotif is deprecated.	PdfStateDown	GGSN

Description:

```
A notification of this type is generated when PDF        connection goes DOWN.
```

Default Message:

Add default message here.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPdfServerAddrType	This object specifies the type of IP address of the PDF server.
cGgsnPdfServerAddr	This object specifies the IP address of the PDF server. The type of this address is specified by the object cGgsnPdfServerAddrType.

Go Top

SECTION 5.62

Trap: cGgsnPdfStateUpNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

PdfStateUp	Trap	Event	No	Warning	The cGgsnPdfStateUpNotif is deprecated.	PdfStateUp	GGSN

Description:

```
A notification of this type is generated when PDF        connection comes UP.
```

Default Message:

Add default message here.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPdfServerAddrType	This object specifies the type of IP address of the PDF server.
cGgsnPdfServerAddr	This object specifies the IP address of the PDF server. The type of this address is specified by the object cGgsnPdfServerAddrType.

Go Top

SECTION 5.63

Trap: cGgsnNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWNotification	Trap	Event	No	Warning	The cGgsnNotification is deprecated.	GWNotification	GGSN

Description:

```
This notification indicates the occurrence of a GGSN        related alarm. If and when additional useful information
is available for specific types of alarms, then that
information may be appended to the end of the
notification in additional varbinds.
```

Default Message:

Add default message here.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnHistNotifType	This object indicates the type of notification.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).

cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

Go Top

SECTION 5.64

Trap: ciscoIpLocalPoolInUseAddrNoti

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	GGSN
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold abated. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	GGSN
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	GGSN

Description:

A notification indicating that number of used addresses of an IP local pool exceeded the threshold value indicated by cIpLocalPoolStatInUseAddrThldHi.

Default Message:

$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIpLocalPoolStatFreeAddrs	The number of IP addresses available for use in this IP local pool.
cIpLocalPoolStatInUseAddrs	The number of IP addresses being used in this IP local pool.

Go Top

SECTION 5.65

Trap: ciscoTap2MIBActive

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MIBActive	Trap	Event	No	Informational	$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.	Tap2MIBActive	GGSN

Description:

```
This Notification is sent when an intercepting router or        switch is first capable of intercepting a packet corresponding
to a configured data stream. The value of the corresponding
cTap2StreamType which identifies the actual intercept stream
type is included in this notification.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.  Filter
installation can take a long period of time, during which call
progress may be delayed.
```

Default Message:

$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 5.66

Trap: ciscoTap2MediationDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .	Tap2MediationDebug	GGSN

Description:

```
When there is intervention needed due to some events related        to entries configured in cTap2MediationTable, the device
notifies the manager of the event.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.
```

Default Message:

$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable

	does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 5.67

Trap: ciscoTap2StreamDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2StreamDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId	Tap2StreamDebug	GGSN

Description:

```
When there is intervention needed due to some events related       to entries configured in cTap2StreamTable, the device
notifies the manager of the event.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.
```

Default Message:

$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId.br>

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.
cTap2DebugStreamId	The value of this object is that of cTap2StreamIndex of an entry in cTap2StreamTable. This object along with cTap2DebugMediationId identifies an entry in cTap2StreamTable. The value of this object may be zero, in which this debug message is regarding a Mediation Device, but not a particular stream. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2StreamTable fails.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 5.68

Trap: ciscoTap2Switchover

Name	Source	Type	Auto	Severity	Message Text	Correlation Key	Personalities

			Clear				
Tap2Switchover	Trap	Event	No	Informational	$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.	Tap2Switchover	GGSN

Description:

```
This notification is sent when there is a redundant (standby)        route processor available on the intercepting device and the
current active processor is going down causing standby to
takeover. Note that this notification may be sent by the
intercepting device only when it had a chance to know before it
goes down.
Mediation device when received this notification should assume
that configured intercepts on the intercepting device no longer
exist, when the standby processor takes control. This means that
the Mediation device should again configure the intercepts.
```

Default Message:

$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 5.69

Status: ApnInstanceStateAdded and ApnInstanceStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceState	Poll	Event	No	Normal	APN $ApnDisplayName on gateway $NodeDisplayName added in state Active/ActiveReason.	ApnInstanceState	GGSN
ApnInstanceState	Poll	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName added in state $ApnInstanceState/$ApnInstanceStateReason.	ApnInstanceState	GGSN
ApnInstanceState	Poll	Event	No	Normal	APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to Active/ActiveReason.	ApnInstanceState	GGSN
ApnInstanceState	Poll	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to $ApnInstanceState/$ApnInstanceStateReason.	ApnInstanceState	GGSN

Description:

The ApnInstanceStateAdded and ApnInstanceStateChanged status eventsprovide information when an ApnInstance object is added to the MWTM object model or when MWTM detects that the state of an ApnInstance has changed. An ApnInstance is defined as an access-point and accesspoint-name defined on a gateway router. An ApnInstance object is located under the gateway Node object in the MWTM object tree. The value of ApnInstanceState indicates the new state. Possible values of ApnInstanceState include:

- Active - Traffic may flow over this ApnInstance.
- Unknown - The attempt to determine the state of the ApnInstance failed.
- Warning - The ApnInstance is Active however some underlying status contributor of this ApnInstance is not fully functional.
- Deleted - The ApnInstance has been deleted from the object database.

Default Message:

- APN $ApnDisplayName on gateway $NodeDisplayName added in state

$ApnInstanceState/$ApnInstanceStateReason.
- APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to $ApnInstanceState/$ApnInstanceStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
ApnInstanceState	The current state of the ApnInstance.
ApnInstanceStateReason	The current state reason of of the ApnInstance.
ApnInstanceLastState	The previous state of the ApnInstance.

Operational Information:

See also:

Go Top

SECTION 5.70

Status: ApnStateAdded and ApnStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnState	Poll	Event	No	Normal	APN $ApnDisplayName added in state Active/ActiveReason.	ApnState	GGSN
ApnState	Poll	Event	No	Informational	APN $ApnDisplayName added in state $ApnState/$ApnStateReason.	ApnState	GGSN
ApnState	Poll	Event	No	Normal	APN $ApnDisplayName changed state from $ApnLastState to Active/ActiveReason.	ApnState	GGSN
ApnState	Poll	Event	No	Informational	APN $ApnDisplayName changed state from $ApnLastState to $ApnState/$ApnStateReason.	ApnState	GGSN

Description:

The ApnStateAdded and ApnStateChanged status events provideinformation when an Apn object is added to the MWTM object model or when MWTM detects that the state of an Apn has changed. An Apn is defined as an aggregation of a set of ApnInstance objects defined across a set of gateway routers. An Apn object is located as a top level object in the MWTM object tree. The value of ApnState indicates the new state.
Possible values of ApnState include:

- Active - Traffic may flow over this Apn.
- Warning - The Apn is Active however one or more of its constituent ApnInstances is not fully functional.
- Deleted - The Apn has been deleted from the object database.

Default Message:

- Apn $ApnDisplayName added in state $ApnState/$ApnStateReason.
- Apn $ApnDisplayName changed state from $ApnLastState to $ApnState/$ApnStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
ApnState	The current state of the Apn.
ApnStateReason	The current state reason of of the Apn.
ApnLastState	The previous state of the Apn.

Operational Information:

See also:

Go Top

SECTION 5.71

UserAction: ApnInstanceIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceIgnoredSet	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.	ApnInstanceIgnoredSet	GGSN

Description:

The ApnInstanceIgnoredSet UserAction event provides information when a ApnInstance's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the ApnInstance in the aggregation algorithm in determining the state of a Node or Apn. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The ApnInstance is to be excluded from state aggregation.
- False - The ApnInstance is to be included in state aggregation.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
ApnInstanceState	The current state of the ApnInstance.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the ApnInstances which are currently ignored select the ApnInstance folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 5.72

UserAction: ApnIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnIgnoredSet	User Action	Event	No	Informational	APN $ApnDisplayName ignore flag is set to $IgnoredFlag by $User.	ApnIgnoredSet	GGSN

Description:

The ApnIgnoredSet UserAction event provides information when a Apn's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the Apn in the aggregation algorithm in determining the state of higher level objects. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The Apn is to be excluded from state aggregation.

False - The Apn is to be included in state aggregation.

Default Message:

APN $ApnDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
ApnState	The current state of the Apn.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the Apns which are currently ignored select the Apn folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 5.73

UserAction: ApnInstanceUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceUserDataUpdated	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName edited by user $User.	ApnInstanceUserDataUpdated	GGSN

Description:

The ApnInstanceUserDataUpdated UserAction event provides information when a ApnInstance object's user data has been updated by a MWTM user.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName edited by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
User	The user who requested the ApnInstance's data be updated.

Operational Information:

The fields that can be updated for a ApnInstance include:

- The ApnInstance's notes data used for communicating installation dependent information about a ApnInstance.

Go Top

SECTION 5.74

UserAction: ApnUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnUserDataUpdated	User Action	Event	No	Informational	APN $ApnDisplayName edited by user $User.	ApnUserDataUpdated	GGSN

Description:

The ApnUserDataUpdated UserAction event provides information when a Apn object's user data has been updated by a MWTM user.

Default Message:

APN $ApnDisplayName edited by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
User	The user who requested the Apn's data be updated.

Operational Information:

The fields that can be updated for a Apn include:

- The Apn's notes data used for communicating installation dependent information about a Apn.

Go Top

SECTION 5.75

UserAction: ApnInstanceDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceDeleted	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName deleted by user $User.	ApnInstanceDeleted	GGSN

Description:

The ApnInstanceDeleted UserAction event provides information when a ApnInstanceobject's deletion from the MWTM object model database is requested.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName deleted by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
User	The user who requested the ApnInstance's data be deleted.

Operational Information:

- The deletion of a ApnInstance can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 5.76

UserAction: ApnDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnDeleted	User Action	Event	No	Informational	APN $ApnDisplayName deleted by user $User.	ApnDeleted	GGSN

Description:

The ApnDeleted UserAction event provides information when a Apnobject's deletion from the MWTM object model database is requested.

Default Message:

APN $ApnDisplayName deleted by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
User	The user who requested the Apn's data be deleted.

Operational Information:

- The deletion of a Apn can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 6.1

Trap: mipAuthFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
mipAuthFailure	Trap	Alarm	No	Warning	$NodeDisplayName - A mobile authentication request failed. Reason: $mipSecRecentViolationReason[1]. Violator: $mipSecViolatorAddress .	mipAuthFailure	HA

Description:

```
The mipAuthFailure indicates that the Mobile IP
entity has an authentication failure when it validates
the mobile Registration Request or Reply.
Implementation of this trap is optional.
```

Default Message:

$NodeDisplayName - A mobile authentication request failed.
Reason: $mipSecRecentViolationReason[1]. Violator:
$mipSecViolatorAddress .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

mipSecViolatorAddress	Violator's IP address. The violator is not necessary in the mipSecAssocTable.
mipSecRecentViolationSPI	SPI of the most recent security violation for this peer. If the security violation is due to an identification mismatch, then this is the SPI from the Mobile-Home Authentication Extension. If the security violation is due to an invalid authenticator, then this is the SPI from the offending authentication extension. In all other cases, it should be set to zero.
mipSecRecentViolationIDLow	Low-order 32 bits of identification used in request or reply of the most recent security violation for this peer.
mipSecRecentViolationIDHigh	High-order 32 bits of identification used in request or reply of the most recent security violation for this peer.
mipSecRecentViolationReason	Reason for the most recent security violation for this peer.

Go Top

SECTION 6.2

Trap: ciscoSlbDfpCongestionAbate

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SlbDfpCongestionChange	Trap	Alarm	Yes	Normal	$NodeDisplayName - The SLB DFP value $cslbcProcessorDfpValDfpValue is above the abate threshold $cslbcDfpCongestionAbateThreshold. The system is not congested.	SlbDfpCongestionChange	HA
SlbDfpCongestionChange	Trap	Alarm	Yes	Major	$NodeDisplayName - The SLB DFP value $cslbcProcessorDfpValDfpValue is below the onset threshold $cslbcDfpCongestionOnsetThreshold. The system is congested. Congestion action: $cslbcDfpCongestionThresholdType	SlbDfpCongestionChange	HA
SlbDfpCongestionChange	Poll	Alarm	Yes	Normal	$NodeDisplayName - The SLB DFP value $cslbcProcessorDfpValDfpValue is above the abate threshold $cslbcDfpCongestionAbateThreshold. The system is not congested.	SlbDfpCongestionChange	HA
SlbDfpCongestionChange	Poll	Alarm	Yes	Major	$NodeDisplayName - The SLB DFP value $cslbcProcessorDfpValDfpValue is below the onset threshold $cslbcDfpCongestionOnsetThreshold. The system is congested. Congestion action: $cslbcDfpCongestionThresholdType	SlbDfpCongestionChange	HA

Description:

This event is created when the SLB DFP value is above the abate threshold. The SLB DFP system is not congested.

Default Message:

$NodeDisplayName - The SLB DFP value $cslbcProcessorDfpValDfpValue is above the abate threshold $cslbcDfpCongestionAbateThreshold. The system is not congested.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cslbcDfpCongestionThresholdType	This object is used to inform the type of congestion that has occured. Type of congestion can be one of the following reject abort redirect drop This textual convention defines valid value of the congestion type. The valid congestion type are reject - Incoming registration requests will be rejected. abort - Registration Request being processed will be aborted. redirect - Redirect incoming registration requests to another HA. drop - Drop existing idle Mobile IP bindings. A mobile IP binding is a record present with the server that associates the home address given to the mobile node by its Home

	network with the Care of address granted to it by the Foreign network while it is roaming.
cslbcProcessorDfpValDescription	This element contains the description for the congestion configured on for processor.
cslbcProcessorDfpValDfpValue	This object indicates DFP value for the processor
cslbcDfpCongestionAbateThreshold	This object is used to detect decongestion state. When the DFP level of the system rises above this value, the system is marked as decongested. This value is same for all processors.
cslbcProcessorDfpValPhysicalIndex	This element contains the index of the physical entity or identifier of the processor for which the DFP value is maintained.

Go Top

SECTION 6.3

Trap: crRadiusServerRTTHiNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RadiusServerRTT	Trap	Alarm	Yes	Warning	$NodeDisplayName - Radius Server $crRadiusServerAddr/$crRadiusServerAuthPort - The current server round-trip time is greater than or equal to the high threshold $crRadiusServerRTTThldHi.	RadiusServerRTT	HA
RadiusServerRTT	Trap	Alarm	Yes	Normal	$NodeDisplayName - Radius Server $crRadiusServerAddr/$crRadiusServerAuthPort - The current server round-trip time is less than or equal to the low threshold $crRadiusServerRTTThldNorm.	RadiusServerRTT	HA

Description:

This event indicates that the current server round-trip time is greater than or equal to its rising threshold.

Default Message:

$NodeDisplayName - Radius Server $crRadiusServerAddr/ $crRadiusServerAuthPort - The current server round-trip time is greater than or equal to the high threshold $crRadiusServerRTTThldHi.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
crRadiusServerRTTThldHi	This object represents the high threshold on the round-trip time of RADIUS authentication messages. This is measured as a percentage of configured round-trip time as per RFC-2865. If the round-trip time is greater than or equal to this threshold, the agent generates the crRadiusServerRTTHiNotif notification. The value configured through this object should never be smaller than that configured through crRadiusServerRTTThldNorm.
crRadiusServerAddr	The address of the RADIUS Server.
crRadiusServerAuthPort	This is the destination UDP port number to which RADIUS authentication messages should be sent. The RADIUS server will not be used for authentication if this port number is 0.
crRadiusServerIndex	An arbitrary integer value, greater than zero, and less than and equal to crRadiusServerTableMaxEntries, which identifies a RADIUS Server in this table. The value of this object must be persistent across reboots/reinitialization of the device.

Go Top

SECTION 6.4

Trap: crRadiusServerRetransHiNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RadiusServerRetrans	Trap	Alarm	Yes	Warning	$NodeDisplayName - Radius Server $crRadiusServerAddr/$crRadiusServerAuthPort - The current number of server retransmissions are greater than or equal to the high threshold $crRadiusServerRetransThldHi.	RadiusServerRetrans	HA
RadiusServerRetrans	Trap	Alarm	Yes	Normal	$NodeDisplayName - Radius Server $crRadiusServerAddr/$crRadiusServerAuthPort - The current number of server retransmissions are less than or equal to the low threshold $crRadiusServerRetransThldNorm.	RadiusServerRetrans	HA

Description:

This event indicates that the current number of server retransmissions is greater than or equal to its rising threshold.

Default Message:

$NodeDisplayName - Radius Server $crRadiusServerAddr/ $crRadiusServerAuthPort - The current number of server retransmissions are greater than or equal to the high threshold $crRadiusServerRetransThldHi.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
crRadiusServerRetransThldHi	This object represents the high threshold on the retransmitted RADIUS authentication messages per session. This is measured as a percentage of crRadiusRetransmits. If the number of retransmits is greater than or equal to this threshold, the agent generates the crRadiusServerRetransHiNotif notification. The value configured through this object should never be smaller than that configured through crRadiusServerRetransThldNorm.
crRadiusServerAddr	The address of the RADIUS Server.
crRadiusServerAuthPort	This is the destination UDP port number to which RADIUS authentication messages should be sent. The RADIUS server will not be used for authentication if this port number is 0.
crRadiusServerIndex	An arbitrary integer value, greater than zero, and less than and equal to crRadiusServerTableMaxEntries, which identifies a RADIUS Server in this table. The value of this object must be persistent across reboots/reinitialization of the device.

Go Top

SECTION 6.5

Status: HaMobilityBindings

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
HaMobilityBindings	Poll	Alarm	Yes	Warning	$NodeDisplayName - Current attached mobile devices: $cmiHaRegTotalMobilityBindings. Max Allowed: $cmiHaMaximumBindings. Utilization $HaMobilityBindingsPercent%.	HaMobilityBindings	HA
HaMobilityBindings	Poll	Alarm	Yes	Major	$NodeDisplayName - Current attached mobile devices: $cmiHaRegTotalMobilityBindings. Max Allowed: $cmiHaMaximumBindings. Utilization $HaMobilityBindingsPercent%.	HaMobilityBindings	HA
HaMobilityBindings	Poll	Alarm	Yes	Critical	$NodeDisplayName - Current attached mobile devices: $cmiHaRegTotalMobilityBindings. Max Allowed: $cmiHaMaximumBindings. Utilization $HaMobilityBindingsPercent%.	HaMobilityBindings	HA
HaMobilityBindings	Poll	Alarm	Yes	Normal	$NodeDisplayName - Current attached mobile devices: $cmiHaRegTotalMobilityBindings. Max Allowed: $cmiHaMaximumBindings. Utilization $HaMobilityBindingsPercent%.	HaMobilityBindings	HA

Description:

This status alarm is generated whenthe ratio of attached mobile devices (cmiHaRegTotalMobilityBindings) relative to the maximum allowed (cmiHaMaximumBindings) causes HaMobilityBindingState to transitions between the Critical, Major, Warning, and Normal states.

Default Message:

- $NodeDisplayName - Current attached mobile devices: $cmiHaRegTotalMobilityBindings. Max Allowed: $cmiHaMaximumBindings. Utilization $HaMobilityBindingsPercent%.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
HaMobilityBindingState	Indicates the utilization of the HomeAgent. • Critical: 100% utilized. No more mobile devices can bind to the HomeAgent. • Major: Between 90% to 100% utilized [90%-100%). • Warning: Between 80% to 90% utilized [80%-90%). • Normal: Less than 80% utilized [0%-80%). In order for the state to transistion from a higher severity state to a lower severity state the utilization of the HomeAgent must fall at least one percent below the current level. So in order to transition from 'Major' to 'Warning' the utilization must fall to less than 89%.
cmiHaRegTotalMobilityBindings	The current number of mobile devices bound to the HomeAgent.
cmiHaMaximumBindings	Maximum No. of Registrations allowed in the HomeAgent.
HaMobilityBindingsPercent	The ratio of cmiHaRegTotalMobilityBindings / cmiHaMaximumBindings expressed as a percent.

Operational Information:

Go Top

SECTION 6.6

Status: AddressesInUsePercentThreshold

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AddressesInUsePercentThreshold	Poll	Alarm	Yes	Critical	$NodeDisplayName - For IP local pool $cIpLocalPoolName $AddressesInUsePercent% of the addresses are in use. The total number of addresses is $TotalAddressesInPool.	AddressesInUsePercentThreshold	HA
AddressesInUsePercentThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - For IP local pool $cIpLocalPoolName $AddressesInUsePercent% of the addresses are in use. The total number of addresses is $TotalAddressesInPool.	AddressesInUsePercentThreshold	HA
AddressesInUsePercentThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - For IP local pool $cIpLocalPoolName $AddressesInUsePercent% of the addresses are in use. The total number of addresses is $TotalAddressesInPool.	AddressesInUsePercentThreshold	HA
AddressesInUsePercentThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - For IP local pool $cIpLocalPoolName $AddressesInUsePercent% of the addresses are in use. The total number of addresses is $TotalAddressesInPool.	AddressesInUsePercentThreshold	HA

Description:

This status alarm is generated, for a given IP local pool, when thevalue of AddressesInUsePercent causes AddressUseState to transition between the
Critical, Major, Warning, and Normal
states.

Default Message:

- $NodeDisplayName - For IP local pool $cIpLocalPoolName $AddressesInUsePercent% of the addresses are in use. The total number of addresses is $TotalAddressesInPool.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIpLocalPoolName	An arbitrary non-empty string that uniquely identifies the IP local pool. This name must be unique among all the local IP pools even when they belong to different pool groups.
cIpLocalPoolStatInUseAddrs	The number of IP addresses being used in this IP local pool.
cIpLocalPoolStatFreeAddrs	The number of IP addresses available for use in this IP local pool.
TotalAddressesInPool	The number of IP addresses in the pool. This value is equivalent to cIpLocalPoolStatInUseAddrs + cIpLocalPoolStatFreeAddrs.
AddressesInUsePercent	The percentage of IP addresses used in the pool.
AddressUseState	Indicates the utilization of the IP local pool. • Critical: 100% utilized. There are no more free addresses in the pool. • Major: Between 90% to 100% utilized [90%-100%). • Warning: Between 80% to 90% utilized [80%-90%). • Normal: Less than 80% utilized [0%-80%). In order for the state to transistion from a higher severity state to a lower severity state the utilization of the pool must fall at least one percent below the current level. So in order to transition from 'Major' to 'Warning' the utilization must fall to less than 89%.

Operational Information:

Go Top

SECTION 6.7

Trap: ciscoIpLocalPoolInUseAddrNoti

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	HA
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold abated. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	HA
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	HA

Description:

A notification indicating that number of used addresses of an IP local pool exceeded the threshold value indicated by cIpLocalPoolStatInUseAddrThldHi.

Default Message:

$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIpLocalPoolStatFreeAddrs	The number of IP addresses available for use in this IP local pool.
cIpLocalPoolStatInUseAddrs	The number of IP addresses being used in this IP local pool.

Go Top

SECTION 6.8

Trap: cmiHaMnRegReqFailed

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
cmiHaMnRegReqFailed	Trap	Event	No	Informational	$NodeDisplayName - Registration for MN $cmiNtRegCOA/$cmiNtRegHomeAddress/$cmiNtRegNAI failed. Reason: $cmiNtRegDeniedCode[1]	cmiHaMnRegReqFailed	HA

Description:

```
The MN registration request failed notification.
This notification is sent when the registration
request from MN is rejected by Home Agent.
```

Default Message:

$NodeDisplayName - Registration for MN $cmiNtRegCOA/$cmiNtRegHomeAddress/$cmiNtRegNAI failed. Reason: $cmiNtRegDeniedCode[1]

Message Substitution Variables:

Common	Substitution variables common to all traps.

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cmiNtRegCOAType	Represents the type of the address stored in cmiHaRegMnCOA.
cmiNtRegCOA	The Mobile Node's Care-of address.
cmiNtRegHAAddrType	Represents the type of the address stored in cmiHaRegMnHa.
cmiNtRegHomeAgent	The Mobile Node's Home Agent address.
cmiNtRegHomeAddressType	Represents the type of the address stored in cmiHaRegRecentHomeAddress.
cmiNtRegHomeAddress	Home (IP) address of visiting mobile node.
cmiNtRegNAI	The identifier associated with the mobile node.
cmiNtRegDeniedCode	The Code indicating the reason why the most recent Registration Request for this mobile node was rejected by the home agent.

Go Top

SECTION 6.9

Trap: cmiHaMaxBindingsNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
cmiHaMaxBindingsNotif	Trap	Event	No	Major	$NodeDisplayName - Homeagent has reached the maximum number of bindings. Current bindings: $cmiHaRegTotalMobilityBindings / Max bindings: $cmiHaMaximumBindings	cmiHaMaxBindingsNotif	HA

Description:

The Homeagent total registrations reached maximum Bindings
This notification is sent when the registration
request from MN is rejected by Home Agent .

Default Message:

$NodeDisplayName - Homeagent has reached the maximum number of bindings. Current bindings: $cmiHaRegTotalMobilityBindings / Max bindings: $cmiHaMaximumBindings

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cmiHaRegTotalMobilityBindings	The current number of entries in haMobilityBindingTable. haMobilityBindingTable contains the home agent's mobility binding list. The home agent updates this table in response to registration events from mobile nodes.

cmiHaMaximumBindings	Maximum No. of Registrations allowed in the HomeAgent.

Go Top

SECTION 7.1

Trap: cerent454Events

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
cerent454Event	Trap	Alarm	Yes	Minor	$NodeDisplayName - A $TrapName alarm (NSA) occurred on $cerent454AlarmObjectName.	cerent454Event	IP-RAN
cerent454Event	Trap	Alarm	Yes	Major	$NodeDisplayName - A $TrapName alarm (NSA) occurred on $cerent454AlarmObjectName.	cerent454Event	IP-RAN
cerent454Event	Trap	Alarm	Yes	Critical	$NodeDisplayName - A $TrapName alarm (NSA) occurred on $cerent454AlarmObjectName.	cerent454Event	IP-RAN
cerent454Event	Trap	Alarm	Yes	Minor	$NodeDisplayName - A $TrapName alarm (SA) occurred on $cerent454AlarmObjectName.	cerent454Event	IP-RAN
cerent454Event	Trap	Alarm	Yes	Major	$NodeDisplayName - A $TrapName alarm (SA) occurred on $cerent454AlarmObjectName.	cerent454Event	IP-RAN
cerent454Event	Trap	Alarm	Yes	Minor	$NodeDisplayName - A $TrapName alarm (SA) occurred on $cerent454AlarmObjectName.	cerent454Event	IP-RAN
cerent454Event	Trap	Alarm	Yes	Normal	$NodeDisplayName - A $TrapName alarm cleared on $cerent454AlarmObjectName.	cerent454Event	IP-RAN
cerent454Event	Trap	Alarm	Yes	Minor	$NodeDisplayName - A $TrapName event (SA) occurred on $cerent454AlarmObjectName.	cerent454Event	IP-RAN
cerent454Event	Trap	Event	Yes	Informational	$NodeDisplayName - A $TrapName event (NSA) occurred on $cerent454AlarmObjectName.	cerent454Event	IP-RAN
cerent454Event	Trap	Event	Yes	Informational	$NodeDisplayName - A $TrapName event occurred on $cerent454AlarmObjectName.	cerent454Event	IP-RAN

Description:

The CERENT-454-MIB defines the events and alarms thatare raised by the ONS 15454. MWTM processes each ONS event by creating an MWTM event with a severity that maps to the severity of the ONS event.

Default Message:

A $Enterprise alarm occurred on $ModelRecordFQDN.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
Enterprise	The notification enterprise identifies the name of each event defined in the CERENT-454-MIB. The possible values for this variable are listed in the table below.

alarmUnknown, alarmCutoffIsInManualMode, failureDetectedExternalToTheNE, externalError, excessiveSwitching, terminationFailureSDCC, incomingFailureCondition, alarmIndicationSignal, alarmIndicationSignalLine, alarmIndicationSignalPath, alarmIndicationSignalVT, channelFailureAPS, channelByteFailureAPS, channelProtectionSwitchingChannelMatchFailureAPS, channelAutomaticProtectionSwitchModeMismatchAPS, channelFarEndProtectionLineFailureAPS,	controllerBToShelfSlotCommunicationFailure, interconnectionEquipmentFailureWorkingPayloadBus, interconnectionEquipmentFailureProtectPayloadBus, inhibitSwitchToProtectRequestInEffectOnEquipment, inhibitSwitchToWorkingRequestInEffectOnEquipment, exerciseRingCompleted, exerciseSpanCompleted, spanIsInWaitToRestoreState, exerciseRingFailed, exerciseSpanFailed, farEndLockoutOfProtectionChannelInSpan, manufacturingEepromFailure, replaceableEquipmentIsMissing,

inconsistentAPSCode,
improperAPSCode,
nodeIdMismatch,
channelDefaultKAPS,
connectionLoss,
bipolarViolation,
carrierLossOnTheLAN,
concatenationErrorSTS,
excessCollisionsOnTheLAN,

facilityCriticalAlarmCausedByDS3FacilityFailure,
farEndAIS,
farEndMultipleDS1LOSDetectedOnDS3,

farEndDS1EqptFailNonServiceAffecting,
farEndDS1EqptFailServiceAffecting,
farEndSingleDS1LOS,

farEndDS3EqptFailNonServiceAffecting,
farEndDS3EqptFailServiceAffecting,

farEndCmnEqptFailNonServiceAffecting,
farEndIDLE,
farEndLOS,
farEndLOF,
farEndBlockError,
idleConditionDS3,
lossOfFrame,
lossOfPointer,
lossOfPointerPath,
lossOfPointerVT,
lossOfSignal,
outOfFrame,

pathSelectorInabilityToSwitchToAValidSignal,
remoteAlarmIndication,
remoteFailureIndication,
remoteFailureIndicationLine,
remoteFailureIndicationPath,
remoteFailureIndicationVT,

facilityHasPassedBERThresholdForSignalDegrade,
severelyErroredFrame,

facilityHasPassedBERThresholdForSignalFailure,
signalLabelMismatchFailure,
payloadDefectIndication,
payloadDefectIndicationPath,
payloadLabelMismatchPath,

signalLabelMismatchFailurePayloadLabelMismatchVT,
unequippedPath,

signalLabelMismatchFailureUnequippedVT,
lossOfTimingOnSynchronizationLink,

lossOfTimingOnAllSpecifiedSynchronizationLinks,

lossOfTimingOnPrimarySynchronizationLink,

lossOfTimingOnSecondarySynchronizationLink,

lossOfTimingOnThirdSynchronizationLink,

lossOfTimingOnFourthSynchronizationLink,

lossOfTimingOnFifthSynchronizationLink,

lossOfTimingOnSixthSynchronizationLink,

failedToReceiveSynchronizationStatusMessage,
softwareDownloadFailed,
extraTrafficDropped,
pktLossDueToOversubscribedXmit,
pktLossDueToOversubscribedRcv,
excessiveEthernetFlowCtlXmited,
excessiveEthernetFlowCtlRecvd,
transportLayerFailure,
etherHdgeInternalFifoUnderrun,

synchronizationReferenceFrequencyOutOfBounds,
ntpOrSntpHostFailure,
peerCardNotResponding,

alarmsAndEventsSuppressedForThisObject,
ds3FrameFormatMismatch,

regenerationSectionTraceIdentifierMismatch,

sdhMultiplexSectionAlarmIndicationSignal,

sdhMultiplexSectionRemoteFailureIndication,

sdhHighOrderTraceIdentifierMismatch,

sdhAdministrationUnitAlarmIndicationSignal,
sdhAdministrationUnitLossofPointer,
sdhSLMFHighOrderUnequippedPath,
sdhSLMFHighOrderPathLabelMismatch,

sdhHighOrderRemoteFailureIndication,
sdhTributaryUnitLossofPointer,

sdhTributaryUnitAlarmIndicationSignal,
sdhSLMFLowOrderUnequippedPath,
sdhSLMFLowOrderPathLabelMismatch,
sdhLowOrderTraceIdentifierMismatch,
sdhLowOrderRemoteFailureIndication,
g811PrimaryReferenceClockTraceable,
g812TransitNodeClockTraceable,
g812LocalNodeClockTraceable,

g813SynchronousEqptTimingSourceTraceable,
loopbackDueToFEACCommandE1,
loopbackCommandSentToFarEndE1,
loopbackDueToFEACCommandE3,
farEndMultipleE1LOSDetectedOnE3,

farEndE1EqptFailNonServiceAffecting,
farEndE1EqptFailServiceAffecting,
farEndSingleE1LOS,
farEndE3EqptFailServiceAffecting,
loopbackCommandSentToFarEndE3,

farEndE3EqptFailNonServiceAffecting,
lowVoltBatteryA,
highVoltBatteryA,
lowVoltBatteryB,
highVoltBatteryB,
msspRingOutOfSync,
resynchronizedMSSPTables,
automaticSNCPSwitchCausedByAIS,
automaticSNCPSwitchCausedByLOP,
automaticSNCPSwitchCausedByUneq,
automaticSNCPSwitchCausedByPDI,
automaticSNCPSwitchCausedBySfber,
automaticSNCPSwitchCausedBySdber,
concatenationErrorSTM,
idleConditionE3,
channelMSSPInconsistentAPSCode,
channelMSSPImproperAPSCodeAPS,
channelMSSPNodeIdMismatchAPS,

synchronizationStatusMessagesAreDisabled,

primaryReferenceSourceStratum1Traceable,
synchronizedTraceabilityUnknown,
stratum2Traceable,
transitNodeClockTraceable,
stratum3ETraceable,
stratum3Traceable,
minimumClockTraceableSonet,
stratum4Traceable,
doNotUseForSynchronization,

reservedForNetworkSynchronizationUse,
outgoingFailureCondition,
remoteDefectIndicationLine,
remoteDefectIndicationPath,
freeRunningSynchronizationMode,
holdoverSynchronizationMode,
fastStartSynchronizationMode,
internalHardwareFaultOrFailure,
errorInternalToTheNEDetected,
internalMessageError,
mismatchOfEquipmentAndAttributes,
watchdogTimerTimeout,
softwareFaultOrFailure,
softwareFaultDataIntegrityFault,
programFailure,
controlEquipmentFailure,

controlEquipmentPrimaryNonVolatileBackupMemoryFailure,

cntrlEqptSecondaryNonVolatileBackupMemoryFailed,
controlEquipmentControlBusFailure,
controlEquipmentControlBus1Failure,
controlEquipmentControlBus2Failure,

communicationFailureTCCAToShelfSLOT1,

communicationFailureTCCAToShelfSLOT2,

communicationFailureTCCAToShelfSLOT3,

communicationFailureTCCAToShelfSLOT4,

communicationFailureTCCAToShelfSLOT5,

communicationFailureTCCAToShelfSLOT6,

communicationFailureTCCAToShelfSLOT7,

communicationFailureTCCAToShelfSLOT8,

communicationFailureTCCAToShelfSLOT9,

communicationFailureTCCAToShelfSLOT10,

communicationFailureTCCAToShelfSLOT11,

communicationFailureTCCAToShelfSLOT12,

communicationFailureTCCAToShelfSLOT13,

communicationFailureTCCAToShelfSLOT14,

communicationFailureTCCAToShelfSLOT15,

communicationFailureTCCAToShelfSLOT16,

communicationFailureTCCAToShelfSLOT17,
channelMSSPDefaultKAPS,
channelMSSPConnectionLossAPS,
minimumClockTraceableSDH,
lineIsInWaitToRestoreStateSDH,

passedBERThresholdForSignalDegradeHighOrder,

passedBERThresholdForSignalFailHighOrder,

passedBERThresholdForSignalDegradeLowOrder,

passedBERThresholdForSignalFailLowOrder,

failureToSwitchToProtectionHighOrder,

failureToSwitchToProtectionLowOrder,
a8b10bOutOfSync,
odukAlarmIndicationSignal,
otukAlarmIndicationSignal,
otukSMBackwardDefectIndication,
odukBackwardDefectIndication,
fecUncorrectedWord,
gccTerminationFailure,
otukIncomingAlignmentError,
odukLockedDefectPm,
lossOfMultiFrame,
odukOpenConnectionIndication,
payloadTypeIdentifierMismatch,
odukTrailTraceIdentifierMismatch,
otukTrailTraceIdentifierMismatch,
equipmentHighLaserBias,
equipmentHighLaserTemp,
equipmentHighLaserPeltier,
equipmentHighRxPower,
equipmentHighTxPower,
equipmentHighTransceiverVoltage,
equipmentLowLaserBias,
equipmentLowLaserTemp,
equipmentLowLaserPeltier,
equipmentLowRxPower,
equipmentLowTxPower,
equipmentLowTransceiverVoltage,
equipmentRxLocked,
equipmentSquelched,
equipmentTxLocked,
otukSignalFailure,
odukSignalFailure,
otukSignalDegrade,
odukSignalDegrade,
pluggablePortMissing,
pluggablePortRateMismatch,
pluggablePortSecurityCodeMismatch,
tciNotSelected,
tci1ClockFailure,
odukPMBackwardDefectIndication,
odukTCM1BackwardDefectIndication,
odukTCM2BackwardDefectIndication,
equipmentHighRxTemperature,
equipmentLowRxTemperature,
tci2ClockFailure,
equipmentWavelengthMismatch,
dspCommunicationFailure,
dspFailure,
laserApproachingEndOfLife,
crossconnectLoopback,
adminLogoutOfUser,
userLockedOut,
adminLockoutOfUser,
adminLockoutClear,
invalidLoginUsername,
invalidLoginPassword,

communicationFailureTCCPAToTCCJAprocessor,

communicationFailureTCCBToShelfSLOT1,

communicationFailureTCCBToShelfSLOT2,

communicationFailureTCCBToShelfSLOT3,

communicationFailureTCCBToShelfSLOT4,

communicationFailureTCCBToShelfSLOT5,

communicationFailureTCCBToShelfSLOT6,

communicationFailureTCCBToShelfSLOT7,

communicationFailureTCCBToShelfSLOT8,

communicationFailureTCCBToShelfSLOT9,

communicationFailureTCCBToShelfSLOT10,

communicationFailureTCCBToShelfSLOT11,

communicationFailureTCCBToShelfSLOT12,

communicationFailureTCCBToShelfSLOT13,

communicationFailureTCCBToShelfSLOT14,

communicationFailureTCCBToShelfSLOT15,

communicationFailureTCCBToShelfSLOT16,

communicationFailureTCCBToShelfSLOT17,

communicationFailureTCCPBToTCCJBprocessor,

controlEquipmentControlCommunicationsEquipmentFailure,

controlEquipmentControlProcessorFailure,

controlEquipmentWorkingMemoryFailure,
interconnectionEquipmentFailure,

interconnectionEquipmentFailurePayloadBus1Working,

interconnectionEquipmentFailurePayloadBus2Working,

interconnectionEquipmentFailurePayloadBus3Working,

interconnectionEquipmentFailurePayloadBus4Working,

interconnectionEquipmentFailurePayloadBus5Working,

interconnectionEquipmentFailurePayloadBus6Working,

interconnectionEquipmentFailurePayloadBus7Working,

interconnectionEquipmentFailurePayloadBus8Working,

interconnectionEquipmentFailurePayloadBus9Working,

interconnectionEquipmentFailurePayloadBus10Working,

interconnectionEquipmentFailurePayloadBus11Working,

interconnectionEquipmentFailurePayloadBus12Working,

interconnectionEquipmentFailurePayloadBus1Protect,

invalidLoginLockedOut,
invalidLoginAlreadyLoggedOn,
loginOfUser,
automaticLogoutOfIdleUser,
logoutOfUser,
firewallHasBeenDisabled,
connectionEquipmentMismatch,
disableInactiveUser,
disableInactiveClear,
batteryFailure,
extremeHighVolt,
extremeLowVolt,
highVolt,
lowVolt,
suspendUser,
suspendUserClear,
lineDCCTerminationFailure,

multiplexSectionDCCTerminationFailure,
gigabitEthernetOutOfSync,
sequenceMismatch,
lossOfAlignment,
outOfUseAdministrativeCommand,
outOfUseTransportFailure,
vcatGroupDown,
vcatGroupDegraded,
vcatGroupIncomplete,
alarmIndicationSignalInTX,
remoteAlarmIndicationInTX,
kbyteChannelFailure,
apsInvalidMode,

ipAddressAlreadyInUseWithinTheSameDCCArea,

nodeNameAlreadyInUseWithinTheSameDCCArea,
rearPanelEthernetLinkRemoved,

manualSwitchToProtectResultedInNoTrafficSwitch,

manualSwitchBackToWorkingResultedInNoTrafficSwitch,

forcedSwitchToProtectionResultedInNoTrafficSwitch,

forcedSwitchBackToWorkingResultedInNoTrafficSwitch,

duplicateSerialNumberDetectedOnAPluggableEntity,
lossOfSignalForOpticalChannel,
encapsulationMismatchPath,
encapsulationMismatchVT,
encapsulationMismatchHighOrderPath,
encapsulationMismatchLowOrderPath,
gfpUserPayloadMismatch,

gfpFibreChannelDistanceExtensionMismatch,

gfpFibreChannelDistanceExtensionBufferStarvation,

fibreChannelDistanceExtensionCreditStarvation,
gfpClientSignalFailDetected,
gfpLossOfFrameDelineation,
gfpExtensionHeaderMismatch,
lcasVCGMemberTxSideInADDState,
lcasVCGMemberTxSideInDNUState,
lcasControlWordCRCCheckFailure,
lcasVCGMemberRxSideInFAILState,
signalLossOnDataInterface,
synchronizationLossOnDataInterface,
portFAIL,
unreachablePortTargetPower,
portAddPowerDegradeLow,
portAddPowerDegradeHigh,

interconnectionEquipmentFailurePayloadBus2Protect,

interconnectionEquipmentFailurePayloadBus3Protect,

interconnectionEquipmentFailurePayloadBus4Protect,

interconnectionEquipmentFailurePayloadBus5Protect,

interconnectionEquipmentFailurePayloadBus6Protect,

interconnectionEquipmentFailurePayloadBus7Protect,

interconnectionEquipmentFailurePayloadBus8Protect,

interconnectionEquipmentFailurePayloadBus9Protect,

interconnectionEquipmentFailurePayloadBus10Protect,

interconnectionEquipmentFailurePayloadBus11Protect,

interconnectionEquipmentFailurePayloadBus12Protect,

interconnectionEqptTimeSlotInterchangeEqptFailure,
equipmentFailure,
equipmentFailureHighTemperature,
equipmentFailureInvalidMACAddress,
equipmentFailureBoardFailure,
equipmentFailureDiagnosticsFailure,

equipmentFailureMediumAccessControl,

facilityTerminationEquipmentFailure,

automaticLaserShutoffDueToHighTemperature,
failureToReleaseFromProtection,

facilityTerminationEquipmentReceiverFailure,

facilityTerminationEquipmentTransmitFailure,

facilityTerminationEquipmentReceiverMissing,

facilityTerminationEquipmentTransmitterMissing,
failureToSwitchToProtection,
failureToSwitchToProtectionRing,
failureToSwitchToProtectionSpan,
failureToSwitchToProtectionPath,
failureOfCoolingFanTray,
equipmentUnitPlugIn,
powerFailureDetectedInternalToNE,
powerFailureFuseAlarm,
synchronizationUnitFailure,

synchronizationSwitchingEquipmentFailure,
equipmentUnitUnplug,
loopback,
loopbackDueToFEACCommandDS1,
loopbackCommandSentToFarEndDS1,
loopbackDueToFEACCommandDS3,
loopbackCommandSentToFarEndDS3,
loopbackDueToFarEndCommandDS2,
loopbackCommandSentToFarEndDS2,
loopbackFacility,
loopbackNetwork,
loopbackTerminal,
manuallyCausedAbnormalCondition,
newRootDiscoveredInBridgedNetwork,

topologyChangeDiscoveredInBridgedNetwork,
normalCondition,
portAddPowerFailLow,
portAddPowerFailHigh,
automaticWDMANSFinished,
incomingOverheadSignalAbsent,
opticalSafetyRemoteInterlockOn,

automaticPowerControlCorrectionSkipped,
apcCannotSetValueDueToRangeLimits,

farEndManualSwitchBackToWorkingSpan,

farEndForcedSwitchBackToWorkingSpan,

universalTransponderModuleHardwareFailure,

universalTransponderModuleCommunicationFailure,
pluginModuleRangeSettingsMismatch,

automaticPowerControlTerminatedOnManualRequest,
oduk1AlarmIndicationSignal,
oduk2AlarmIndicationSignal,
oduk3AlarmIndicationSignal,
oduk4AlarmIndicationSignal,

temperatureReadingMismatchBetweenSCCards,

voltageReadingMismatchBetweenSCCards,

alarmsSuppressedOnOutOfGroupVCATMember,
blsrSoftwareVersionMismatch,
optimized1Plus1APSPrimaryFacility,

optimized1Plus1APSPrimarySectionMismatch,

optimized1Plus1APSInvalidPrimarySection,
compositeClockHighLineVoltage,

berThresholdExceededForSignalDegradeVT,

berThresholdExceededForSignalFailureVT,
spanLengthOutOfRange,
vtPathTraceIdentifierMismatch,
equipmentPowerFailureAtConnectorA,
equipmentPowerFailureAtConnectorB,

equipmentPowerFailureAtReturnConnectorA,

equipmentPowerFailureAtReturnConnectorB,
ospfHelloFail,

enhancedRemoteFailureIndicationPathServer,

enhancedRemoteFailureIndicationPathConnectivity,

enhancedRemoteFailureIndicationPathPayload,
securityIntrusionIncorrectPassword,
securityIntrusionIncorrectUsername,
odukAlarmIndicationSignalTCM1,
odukAlarmIndicationSignalTCM2,
odukLockedDefectTCM1,
odukLockedDefectTCM2,
otukLossOfFrame,
odukOpenConnectionIndicationTCM1,
odukOpenConnectionIndicationTCM2,

odukTrailTraceIdentifierMismatchTCM1,

odukTrailTraceIdentifierMismatchTCM2,
odukSignalFailureTCM1,
odukSignalFailureTCM2,
odukSignalDegradeTCM1,

embeddedOperationsChannelFailureLinkDown,
peerStateMismatch,
proceduralError,
proceduralErrorImproperRemoval,
proceduralErrorDuplicateNodeID,
proceduralErrorBLSROutOfSync,
resynchronizedBLSRTables,
protectionUnitNotAvailable,

performanceMonitorThresholdCrossingAlert,

occurrenceOfAProtectionSwitchingEvent,

recoveryOrServiceProtectionActionHasBeenInitiated,
automaticSystemReset,
automaticUPSRSwitchCausedByAIS,
automaticUPSRSwitchCausedByLOP,
automaticUPSRSwitchCausedByUneq,
automaticUPSRSwitchCausedByPDI,
automaticUPSRSwitchCausedBySfber,
automaticUPSRSwitchCausedBySdber,
coldRestart,

workingFacilityOrEqptForcedSwitchedToWorking,

workingFacilityOrEqptForcedSwitchedToWorkingRing,

workingFacilityOrEqptForcedSwitchedToWorkingSpan,

workingFacilityOrEqptForcedSwitchedProtectionUnit,

workingFacilityOrEqptForcedSwitchedProtectionUnitRing,

workingFacilityOrEqptForcedSwitchedProtectionUnitSpan,

workingFacilityOrEqptForcedSwitchedProtectionUnitPath,
initializationInitiated,
lockoutOfProtection,
lockoutOfProtectionRing,
lockoutOfProtectionSpan,
lockoutOfProtectionPath,
lockoutOfWorking,
lockoutOfWorkingRing,
lockoutOfWorkingSpan,
manualSystemReset,

manualSynchronizationSwitchToInternalClock,

manualSynchronizationSwitchToPrimaryReference,

manualSynchronizationSwitchToSecondReference,

manualSynchronizationSwitchToThirdReference,

manualSynchronizationSwitchToFourthReference,

manualSynchronizationSwitchToFifthReference,

manualSynchronizationSwitchToSixthReference,

manualSwitchOfWorkingFacilityOrEqptToProtectionRing,

manualSwitchOfWorkingFacilityOrEqptToProtectionSpan,

manualSwitchOfWorkingFacilityOrEqptToProtection,

manualSwitchOfWorkingFacilityOrEqptToProtectionUnit,

workingFacilityOrEqptManualSwitchToProtectionUnitRing,

workingFacilityOrEqptManualSwitchToProtectionUnitSpan,
odukSignalDegradeTCM2,
lossOfChannel,
fecMismatch,

timSectionMonitorTraceIdentifierMismatchFailure,
automaticLaserShutdown,

shutterInsertionLossVariationDegradeLow,
opticalChannelDeactivationFailure,

shutterInsertionLossVariationDegradeHigh,
networkTopologyIncomplete,
pluginModuleCommunicationFailure,
opticalNetworkTypeMismatch,
forcedSwitchToPrimaryReference,
forcedSwitchToSecondReference,
forcedSwitchToThirdReference,
forcedSwitchToInternalClock,
industrialHighTemperature,
laserPowerDegradeLow,
automaticPowerControlFailure,
laserPowerDegradeHigh,
automaticPowerControlDisabled,
laserPowerFailureLow,
ringIdMismatch,
laserPowerFailureHigh,
lossOfContinuity,

variableOpticalAttenuatorDegradeLow,

variableOpticalAttenuatorDegradeHigh,

variableOpticalAttenuatorFailureLow,

variableOpticalAttenuatorFailureHigh,
laserBiasDegrade,
laserBiasFailure,
laserTemperatureDegrade,
opticalAmplifierGainDegradeLow,
opticalAmplifierGainDegradeHigh,
opticalAmplifierGainFailureLow,
opticalAmplifierGainFailureHigh,
opticalChannelConnectionFailure,
opticalChannelIncomplete,
opticalChannelActivationFailure,
laserAutoPowerReduction,
caseTemperatureDegrade,
fiberTemperatureDegrade,
shutterFailure,
awgTemperatureDegrade,
awgTemperatureFailure,
awgOverTemperature,
opticalAmplifierInitialization,
awgWarmUp,

incomingSignalLossOnFibreChannelInterface,

incomingSynchronizationLossOnFibreChannelInterface,
outOfFrameDetectedByGFPReceiver,

clientSignalLossFramesDetectedByGFPReceiver,

clientSychronizationLossFramesDetectedByGFPReceiver,
waitToRestore,
extremeHighVoltBatteryA,
extremeLowVoltBatteryA,
extremeHighVoltBatteryB,
extremeLowVoltBatteryB,
iosConfigCopyFailed,
iosConfigCopyInProgress,
signalingUnableToSetupCircuit,

manualSwitchOfWorkingFacilityOrEqptToProtectionPath,
powerFailureRestart,
ringIsSquelchingTraffic,
softwareDownloadInProgress,

synchronizationSwitchToInternalClock,

synchronizationSwitchToPrimaryReference,

synchronizationSwitchToSecondReference,

synchronizationSwitchToThirdReference,

synchronizationSwitchToFourthReference,

synchronizationSwitchToFifthReference,

synchronizationSwitchToSixthReference,
systemReboot,
switchedBackToWorking,
switchedToProtection,
warmRestart,
ringIsInWaitToRestoreState,
manualSwitchRequest,
forcedSwitchRequest,
lockoutSwitchRequest,
rmonHistoriesAndAlarmsReset,
rmonThresholdCrossingAlarm,
alarmsSuppressedByUserCommand,
alarmsSuppressedForMaintenance,
switchingMatrixModuleFailure,
lanConnectionPolarityReversed,

autonomousPerformanceMonitoringReportMessageInhibited,
ioSlotToXCONCommunicationFailure,
traceIdentifierMismatchSTSPath,
nodePowerFailureAtConnectorA,
nodePowerFailureAtConnectorB,
freeMemoryOnCardVeryLow,
freeMemoryOnCardAlmostGone,
exerciseRing,
exerciseSpan,
squelchingPath,
extraTrafficPreempted,
farEndLockoutOfWorkingRing,
farEndLockoutOfWorkingSpan,
farEndLockoutOfProtectionRing,
farEndLockoutOfProtectionAllSpans,

farEndWorkingFacilityForcedToSwitchToProtectionUnitRing,

farEndWorkingFacilityForcedToSwitchToProtectionUnitSpan,

farEndManualSwitchOfWorkingFacilityToProtectionUnitRing,

farEndManualSwitchOfWorkingFacilityToProtectionUnitSpan,
farEndExerciseRing,
farEndExerciseSpan,

farEndBERThresholdPassedForSignalFailureRing,

farEndBERThresholdPassedForSignalFailureSpan,

farEndBERThresholdPassedForSignalDegradeRing,

farEndBERThresholdPassedForSignalDegradeSpan,

channelFarEndProtectionLineSignalDegradeAPS,
ringSwitchIsActiveOnTheEastSide,
ringSwitchIsActiveOnTheWestSide,
errorInStartupConfig,
noStartupConfig,
needToSaveRunningConfig,
invalidAlarm,
rsvpHelloFsmToNeighborDown,

securityInvalidLoginUsernameSeeAuditLog,
databaseBackupFailed,
databaseRestoreFailed,
lMPHelloFsmToControlChannelDown,
lMPNeighborDiscoveryHasFailed,
auditLog80PercentFull,
moduleCommunicationFailure,

auditLog100PercentFullOldestRecordsWillBeLost,
standbyDatabaseOutOfSync,
redundantPowerCapabilityLost,

sdhAdministrationUnitLossOfMultiframe,
sdhSpanIsInWaitToRestoreState,

berThresholdExceededForSignalDegradeLine,

berThresholdExceededForSignalDegradePath,

berThresholdExceededForSignalFailureLine,

berThresholdExceededForSignalFailurePath,

unauthorizedIncomingSignalingRequest

spanSwitchIsActiveOnTheEastSide, spanSwitchIsActiveOnTheWestSide, uniDirectionalFullPassThroughIsActive, biDirectionalFullPassThroughIsActive, kBytePassThroughIsActive, ringIsSegmented, ringTopologyIsUnderConstruction, lockoutOfProtectionAllSpans, farEndOfFiberIsProvisionedWithDifferentRingID, bothEndsOfFiberProvisionedAsEastOrBothAsWest, invalidLoginSeeAuditTrail, autonomousMessagesInhibited, trafficStormLANtemporarilyDisabled, tl1ReptDbchgMessagesInhibited, userIdHasExpired, partialFanFailure, forceSwitchRequestOnRing, forceSwitchRequestOnSpan, lockoutSwitchRequestOnRing, lockoutSwitchRequestOnSpan, manualSwitchRequestOnRing, manualSwitchRequestOnSpan, communicationFailurePeerToPeerSlotControlBusA, communicationFailurePeerToPeerSlotControlBusB, controllerAToShelfSlotCommunicationFailure,	

Go Top

SECTION 7.2

Trap: cpwVcUp

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PWE3VCState	Trap	Alarm	Yes	Normal	PWE3VC $NodeDisplayName/$PWE3VCDisplayName changed state from Down to Active.	PWE3VCState	IP-RAN
PWE3VCState	Trap	Alarm	Yes	Critical	PWE3VC $NodeDisplayName/$PWE3VCDisplayName changed state from Active to Down.	PWE3VCState	IP-RAN
PWE3VCState	Poll	Alarm	Yes	Normal	PWE3VC $NodeDisplayName/$PWE3VCDisplayName added in state Active/ActiveReason.	PWE3VCState	IP-RAN
PWE3VCState	Poll	Alarm	Yes	Normal	PWE3VC $NodeDisplayName/$PWE3VCDisplayName changed state from $PWE3VCLastState to Active/ActiveReason.	PWE3VCState	IP-RAN
PWE3VCState	Poll	Alarm	Yes	Critical	PWE3VC $NodeDisplayName/$PWE3VCDisplayName added in state Down/DownReason.	PWE3VCState	IP-RAN
PWE3VCState	Poll	Alarm	Yes	Warning	PWE3VC $NodeDisplayName/$PWE3VCDisplayName added in state Warning/WarningReason.	PWE3VCState	IP-RAN
PWE3VCState	Poll	Alarm	Yes	Informational	PWE3VC $NodeDisplayName/$PWE3VCDisplayName added in state $PWE3VCState/$PWE3VCStateReason.	PWE3VCState	IP-RAN
PWE3VCState	Poll	Alarm	Yes	Critical	PWE3VC $NodeDisplayName/$PWE3VCDisplayName changed state from $PWE3VCLastState to Down/DownReason.	PWE3VCState	IP-RAN
PWE3VCState	Poll	Alarm	Yes	Warning	PWE3VC $NodeDisplayName/$PWE3VCDisplayName changed state from $PWE3VCLastState to Warning/WarningReason.	PWE3VCState	IP-RAN
PWE3VCState	Poll	Alarm	Yes	Informational	PWE3VC $NodeDisplayName/$PWE3VCDisplayName changed state from $PWE3VCLastState to $PWE3VCState/$PWE3VCStateReason.	PWE3VCState	IP-RAN

Description:

The cpwVcUp event
is created when MWTM receives the cpwVcUp notification.

Default Message:

- PWE3VC $NodeDisplayName/$PWE3VCDisplayName changed state from
  down to active.

Message Substitution Variables:

Node	Substitution variables for Node related data.
cpwVcIndex	Index for the conceptual row identifying a VC within this PW Emulation VC table.
cpwVcPsnType	Set by the operator to indicate the PSN type on which this VC will be carried. Based on this object, the relevant PSN table entries are created in the in the PSN specific MIB modules. For example, if mpls(1) is defined, the agent create an entry in cpwVcMplsTable, which further define the MPLS PSN configuration. Possible values: mpls, l2tp, ip, mplsOverIp, gre, other
cpwVcType	This value indicate the service to be carried over this VC. Possible values: other, frameRelay, atmAal5Vcc, atmTransparent, ethernetVLAN, ethernet, hdlc, ppp, cep, atmVccCell, atmVpcCell, ethernetVPLS, e1Satop, t1Satop, e3Satop, t3Satop, basicCesPsn, basicTdmIp, tdmCasCesPsn, tdmCasTdmIp
cpwVcPeerAddr	This object contains the value of of the peer node address of the PW/PE maintenance protocol entity. This object should contain a value of 0 if not relevant (manual configuration of the VC).
cpwVcID	Used in the outgoing VC ID field within the 'Virtual Circuit FEC Element' when LDP signaling is used or PW ID AVP for L2TP.
cpwVcRemoteIfString	Indicate the interface description string as received by the maintenance protocol, MUST be NULL string if not applicable or not known yet.
cpwVcName	The canonical name assigned to the VC.
cpwVcDescr	A textual string containing information about the VC. If there is no description this object contains a zero length string.

Operational Information:

- If the current state of the PWE3VirtualCircuit is Active no
  additional
  action is necessary.
- When the current state of the PWE3VirtualCircuit is Down this is
  an
  indication that the RtrInterface is operationally down.

Diagnostic Commands:

To display information about the PWE3VirtualCircuits use commands:

show xconnect all

show xconnect pwmib

Go Top

Trap: ospfIfAuthFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfInterfaceAuthenticationFailure	Trap	Alarm	No	Minor	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf received an OSPF packet of type $ospfPacketType from source interface $ospfPacketSrc with a configuration error of type $ospfConfigErrorType. OSPF Router Id is : $ospfRouterId	OspfInterfaceAuthenticationFailure	IP-RAN

Description:

```
An ospfIfAuthFailure trap signifies that a             packet has been received on a non-virtual
interface from a router whose authentication key
or authentication type conflicts with this
router's authentication key or authentication
type.
```

Default Message:

$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf received an OSPF packet of type $ospfPacketType from source interface $ospfPacketSrc with a configuration error of type $ospfConfigErrorType. OSPF Router Id is : $ospfRouterId

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfConfigErrorType	Potential types of configuration conflicts. Used by the ospfConfigError and ospfConfigVirtError traps. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as noError. INTEGER is unknown
ospfPacketType	OSPF packet types. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as nullPacket. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfIfIpAddress	The IP address of this OSPF interface.
ospfAddressLessIf	For the purpose of easing the instancing of addressed and addressless interfaces; this variable takes the value 0 on interfaces with IP addresses and the corresponding value of ifIndex for interfaces having no IP address.
ospfPacketSrc	The IP address of an inbound packet that cannot be identified by a neighbor instance. When

	the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as 0.0.0.0.

Go Top

SECTION 7.4

Trap: ospfIfConfigError

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfInterfaceConfigError	Trap	Alarm	No	Minor	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf received an OSPF packet of type $ospfPacketType from source interface $ospfPacketSrc with a configuration error of type $ospfConfigErrorType.	OspfInterfaceConfigError	IP-RAN

Description:

```
An ospfIfConfigError trap signifies that a            packet has been received on a non-virtual
interface from a router whose configuration
parameters conflict with this router's
configuration parameters.  Note that the event
optionMismatch should cause a trap only if it
prevents an adjacency from forming.
```

Default Message:

$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf received an OSPF packet of type $ospfPacketType from source interface $ospfPacketSrc with a configuration error of type $ospfConfigErrorType.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfConfigErrorType	Potential types of configuration conflicts. Used by the ospfConfigError and ospfConfigVirtError traps. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as noError. INTEGER is unknown
ospfPacketType	OSPF packet types. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as nullPacket. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfIfIpAddress	The IP address of this OSPF interface.
ospfAddressLessIf	For the purpose of easing the instancing of addressed and addressless interfaces; this

	variable takes the value 0 on interfaces with IP addresses and the corresponding value of ifIndex for interfaces having no IP address.
ospfPacketSrc	The IP address of an inbound packet that cannot be identified by a neighbor instance. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as 0.0.0.0.

Go Top

SECTION 7.5

Trap: ospfIfRxBadPacket

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfBadPacketReceived	Trap	Alarm	No	Warning	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf received an OSPF packet of type $ospfPacketType from source interface $ospfPacketSrc that cannot be parsed.	OspfBadPacketReceived	IP-RAN

Description:

```
An ospfIfRxBadPacket trap signifies that an            OSPF packet has been received on a non-virtual
interface that cannot be parsed.
```

Default Message:

$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf received an OSPF packet of type $ospfPacketType from source interface $ospfPacketSrc that cannot be parsed.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfPacketType	OSPF packet types. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as nullPacket. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfIfIpAddress	The IP address of this OSPF interface.
ospfAddressLessIf	For the purpose of easing the instancing of addressed and addressless interfaces; this variable takes the value 0 on interfaces with IP addresses and the corresponding value of ifIndex for interfaces having no IP address.
ospfPacketSrc	The IP address of an inbound packet that cannot be identified by a neighbor instance. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should

	be returned as 0.0.0.0.

Go Top

SECTION 7.6

Trap: ospfIfStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfInterfaceState	Trap	Alarm	Yes	Major	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to down.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to loopback.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to waiting.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to point-to-point.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to designated router.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to backup designated router.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to other designated router.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Poll	Alarm	Yes	Major	$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to down.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Poll	Event	Yes	Informational	$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to loopback.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Poll	Event	Yes	Informational	$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to waiting.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Poll	Alarm	Yes	Normal	$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to point-to-point.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Poll	Alarm	Yes	Normal	$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to designated router.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Poll	Alarm	Yes	Normal	$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to backup designated router.	OspfInterfaceState	IP-RAN
OspfInterfaceState	Poll	Alarm	Yes	Normal	$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf changed state to other designated router.	OspfInterfaceState	IP-RAN

Description:

```
An ospfIfStateChange trap signifies that there            has been a change in the state of a non-virtual
OSPF interface.  This trap should be generated
when the interface state regresses (e.g., goes
from Dr to Down) or progresses to a terminal
state (i.e., Point-to-Point, DR Other, Dr, or
Backup).
```

Default Message:

$NodeDisplayName - OSPF interface $ospfIfState_ospfIfIpAddress/$ospfIfState_ospfAddressLessIf changed state to down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfIfState	The OSPF Interface State. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System.

	By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfIfIpAddress	The IP address of this OSPF interface.
ospfAddressLessIf	For the purpose of easing the instancing of addressed and addressless interfaces; this variable takes the value 0 on interfaces with IP addresses and the corresponding value of ifIndex for interfaces having no IP address.

Go Top

SECTION 7.7

Trap: ospfLsdbApproachingOverflow

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfLinkStateDbOverflow	Trap	Alarm	No	Minor	$NodeDisplayName -- OSPF link state database is 90% full. LSDB size limit: $ospfExtLsdbLimit.	OspfLinkStateDbOverflow	IP-RAN
OspfLinkStateDbOverflow	Trap	Alarm	No	Major	$NodeDisplayName -- OSPF link state database is full. LSDB size limit: $ospfExtLsdbLimit.	OspfLinkStateDbOverflow	IP-RAN

Description:

```
An ospfLsdbApproachingOverflow trap signifies            that the number of LSAs in the router's
link state database has exceeded ninety percent of
ospfExtLsdbLimit.
```

Default Message:

$NodeDisplayName - OSPF link state database is 90% full. LSDB size limit: $ospfExtLsdbLimit.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfExtLsdbLimit	The maximum number of non-default AS-external LSAs entries that can be stored in the link state database. If the value is -1, then there is no limit. When the number of non-default AS-external LSAs in a router's link state database reaches ospfExtLsdbLimit, the router enters overflow state. The router never holds more than ospfExtLsdbLimit non-default AS-external LSAs in its database. OspfExtLsdbLimit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area (i.e., OSPF stub areas and NSSAs are excluded). This object is persistent and when written the entity SHOULD save the change to non-volatile

	storage.

Go Top

SECTION 7.8

Trap: ospfMaxAgeLsa

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfMaxAgeLsa	Trap	Alarm	No	Minor	$NodeDisplayName -- OSPF LSA reached the maximum age. Link state DB entry: Area: $ospfLsdbAreaId, Type: $ospfLsdbType, LsId : $ospfLsdbLsid, Router Id: $ospfLsdbRouterId	OspfMaxAgeLsa	IP-RAN

Description:

```
An ospfMaxAgeLsa trap signifies that one of            the LSAs in the router's link state database has
aged to MaxAge.
```

Default Message:

$NodeDisplayName - OSPF LSA reached the maximum age. Link state DB entry: Area: $ospfLsdbAreaId, Type: $ospfLsdbType, LsId : $ospfLsdbLsid, Router Id: $ospfLsdbRouterId

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfLsdbType	The type of the link state advertisement. Each link state type has a separate advertisement format. Note: External link state advertisements are permitted for backward compatibility, but should be displayed in the ospfAsLsdbTable rather than here. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfLsdbAreaId	The 32-bit identifier of the area from which the LSA was received.
ospfLsdbLsid	The Link State ID is an LS Type Specific field containing either a Router ID or an IP address; it identifies the piece of the routing domain that is being described by the advertisement.
ospfLsdbRouterId	The 32-bit number that uniquely identifies the originating router in the Autonomous System.

Go Top

SECTION 7.9

Trap: ospfNbrRestartHelperStatusChange

			Auto				

Name	Source	Type	Clear	Severity	Message Text	Correlation Key	Personalities
OspfNeighborRestartHelperState	Trap	Alarm	Yes	Informational	$NodeDisplayName -- OSPF neighbor $ospfNbrIpAddr/$ospfNbrAddressLessIndex restart helper state changed. Status: helping, Age: $ospfNbrRestartHelperAge, Exit Reason: $ospfNbrRestartHelperExitReason	OspfNeighborRestartHelperState	IP-RAN
OspfNeighborRestartHelperState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF neighbor $ospfNbrIpAddr/$ospfNbrAddressLessIndex restart helper state changed. Status: not helping, Age: $ospfNbrRestartHelperAge, Exit Reason: $ospfNbrRestartHelperExitReason.	OspfNeighborRestartHelperState	IP-RAN
OspfNeighborRestartHelperState	Poll	Alarm	Yes	Informational	$NodeDisplayName - OSPF neighbor $ospfNbrIpAddr/$ospfNbrAddressLessIndex restart helper state changed. Status: helping	OspfNeighborRestartHelperState	IP-RAN
OspfNeighborRestartHelperState	Poll	Alarm	Yes	Normal	$NodeDisplayName - OSPF neighbor $ospfNbrIpAddr/$ospfNbrAddressLessIndex restart helper state changed. Status: not helping.	OspfNeighborRestartHelperState	IP-RAN

Description:

```
An ospfNbrRestartHelperStatusChange trap signifies that             there has been a change in the graceful restart
helper state for the neighbor.  This trap should be
generated when the neighbor restart helper status
transitions for a neighbor.
```

Default Message:

$NodeDisplayName - OSPF neighbor $ospfNbrIpAddr/$ospfNbrAddressLessIndex restart helper state changed. Status: helping, Age: $ospfNbrRestartHelperAge, Exit Reason: $ospfNbrRestartHelperExitReason

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfNbrRestartHelperStatus	Indicates whether the router is acting as a graceful restart helper for the neighbor. INTEGER is unknown
ospfNbrRestartHelperExitReason	Describes the outcome of the last attempt at acting as a graceful restart helper for the neighbor. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfNbrIpAddr	The IP address that this neighbor is using in its IP source address. Note that, on addressless links, this will not be 0.0.0.0 but the address of another of the neighbor's interfaces.
ospfNbrAddressLessIndex	On an interface having an IP address, zero. On addressless interfaces, the corresponding value of ifIndex in the Internet Standard MIB. On row creation, this can be derived from the instance.
ospfNbrRtrId	A 32-bit integer (represented as a type IpAddress) uniquely identifying the neighboring

	router in the Autonomous System.
ospfNbrRestartHelperAge	Remaining time in current OSPF graceful restart interval, if the router is acting as a restart helper for the neighbor.

Go Top

SECTION 7.10

Trap: ospfNbrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfNeighborState	Trap	Alarm	Yes	Major	$NodeDisplayName -- OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to down.	OspfNeighborState	IP-RAN
OspfNeighborState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to full	OspfNeighborState	IP-RAN
OspfNeighborState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to two-way.	OspfNeighborState	IP-RAN
OspfNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to attempt.	OspfNeighborState	IP-RAN
OspfNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to init.	OspfNeighborState	IP-RAN
OspfNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to exchangeStart.	OspfNeighborState	IP-RAN
OspfNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to exchange.	OspfNeighborState	IP-RAN
OspfNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to loading.	OspfNeighborState	IP-RAN
OspfNeighborState	Poll	Alarm	Yes	Major	$NodeDisplayName - OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to down.	OspfNeighborState	IP-RAN
OspfNeighborState	Poll	Alarm	Yes	Normal	$NodeDisplayName - OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to full	OspfNeighborState	IP-RAN
OspfNeighborState	Poll	Alarm	Yes	Normal	$NodeDisplayName - OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to two-way.	OspfNeighborState	IP-RAN
OspfNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName - OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to attempt.	OspfNeighborState	IP-RAN
OspfNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName - OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to init.	OspfNeighborState	IP-RAN
OspfNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName - OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to exchangeStart.	OspfNeighborState	IP-RAN
OspfNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName - OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to exchange.	OspfNeighborState	IP-RAN
OspfNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName - OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to loading.	OspfNeighborState	IP-RAN

Description:

```
An ospfNbrStateChange trap signifies that             there has been a change in the state of a
non-virtual OSPF neighbor.  This trap should be
generated when the neighbor state regresses
(e.g., goes from Attempt or Full to 1-Way or
Down) or progresses to a terminal state (e.g.,
2-Way or Full).  When an neighbor transitions
from or to Full on non-broadcast multi-access
and broadcast networks, the trap should be
generated by the designated router.  A designated
router transitioning to Down will be noted by
ospfIfStateChange.
```

Default Message:

$NodeDisplayName - OSPF neighbor address $ospfNbrIpAddr/$ospfNbrAddressLessIndex on $ospfNbrRtrId changed state to $ospfNbrState.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfNbrState	The state of the relationship with this neighbor. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfNbrIpAddr	The IP address that this neighbor is using in its IP source address. Note that, on addressless links, this will not be 0.0.0.0 but the address of another of the neighbor's interfaces.
ospfNbrAddressLessIndex	On an interface having an IP address, zero. On addressless interfaces, the corresponding value of ifIndex in the Internet Standard MIB. On row creation, this can be derived from the instance.
ospfNbrRtrId	A 32-bit integer (represented as a type IpAddress) uniquely identifying the neighboring router in the Autonomous System.

Go Top

SECTION 7.11

Trap: ospfNssaTranslatorStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfNssaTranslatorState	Trap	Alarm	No	Warning	$NodeDisplayName -- OSPF area $ospfAreaId NSSA translator state changed to $ospfAreaNssaTranslatorState.	OspfNssaTranslatorState	IP-RAN
OspfNssaTranslatorState	Poll	Alarm	No	Warning	$NodeDisplayName - OSPF area $ospfAreaId NSSA translator state changed to $ospfAreaNssaTranslatorState.	OspfNssaTranslatorState	IP-RAN

Description:

```
An ospfNssaTranslatorStatusChange trap indicates that            there has been a change in the router's ability to
translate OSPF type-7 LSAs into OSPF type-5 LSAs.
This trap should be generated when the translator
status transitions from or to any defined status on
a per-area basis.
```

Default Message:

$NodeDisplayName - OSPF area $ospfAreaId NSSA translator state changed to $ospfAreaNssaTranslatorState.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfAreaNssaTranslatorState	Indicates if and how an NSSA border router is performing NSSA translation of type-7 LSAs into type-5 LSAs. When this object is set to enabled, the NSSA Border router's OspfAreaNssaExtTranslatorRole has been set to always. When this object is set to elected, a candidate NSSA Border router is Translating type-7 LSAs into type-5. When this object is set to disabled, a candidate NSSA border router is NOT translating type-7 LSAs into type-5. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfAreaId	A 32-bit integer uniquely identifying an area. Area ID 0.0.0.0 is used for the OSPF backbone.

Go Top

SECTION 7.12

Trap: ospfRestartStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfRestartState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- OSPF restart status changed. Status: unplanned restart, Interval: $ospfRestartInterval, Exit Reason: $ospfRestartExitReason	OspfRestartState	IP-RAN
OspfRestartState	Trap	Alarm	Yes	Informational	$NodeDisplayName -- OSPF restart status changed. Status: planned restart, Interval: $ospfRestartInterval, Exit Reason: $ospfRestartExitReason	OspfRestartState	IP-RAN
OspfRestartState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF restart status changed. Status: not restarting, Interval: $ospfRestartInterval, Exit Reason: $ospfRestartExitReason	OspfRestartState	IP-RAN
OspfRestartState	Poll	Alarm	Yes	Minor	$NodeDisplayName - OSPF restart status changed. Status: unplanned restart.	OspfRestartState	IP-RAN
OspfRestartState	Poll	Alarm	Yes	Informational	$NodeDisplayName - OSPF restart status changed. Status: planned restart.	OspfRestartState	IP-RAN
OspfRestartState	Poll	Alarm	Yes	Normal	$NodeDisplayName - OSPF restart status changed. Status: not restarting	OspfRestartState	IP-RAN

Description:

```
An ospfRestartStatusChange trap signifies that             there has been a change in the graceful restart
state for the router.  This trap should be
generated when the router restart status
changes.
```

Default Message:

$NodeDisplayName - OSPF restart status changed. Status: unplanned restart/planned restart/not restarting, Interval: $ospfRestartInterval, Exit Reason: $ospfRestartExitReason

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfRestartStatus	Current status of OSPF graceful restart.

	INTEGER is unknown
ospfRestartExitReason	Describes the outcome of the last attempt at a graceful restart. If the value is 'none', no restart has yet been attempted. If the value is 'inProgress', a restart attempt is currently underway. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfRestartInterval	Configured OSPF graceful restart timeout interval. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.

Go Top

SECTION 7.13

Trap: ospfTxRetransmit

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfRetransmit	Trap	Alarm	No	Warning	$NodeDisplayName -- OSPF interface $ospfIfIpAddress/$ospfAddressLessIf retransmitted an OSPF packet of type $ospfPacketType to destination router id $ospfNbrRtrId. Link state DB entry: Type: $ospfLsdbType, LsId: $ospfLsdbLsid, RouterId: $ospfLsdbRouterId	OspfRetransmit	IP-RAN

Description:

```
An ospfTxRetransmit trap signifies than an             OSPF packet has been retransmitted on a
non-virtual interface.  All packets that may be
retransmitted are associated with an LSDB entry.
The LS type, LS ID, and Router ID are used to
identify the LSDB entry.
```

Default Message:

$NodeDisplayName - OSPF interface $ospfIfIpAddress/$ospfAddressLessIf retransmitted an OSPF packet of type $ospfPacketType to destination router id $ospfNbrRtrId. Link state DB entry: Type: $ospfLsdbType, LsId: $ospfLsdbLsid, RouterId: $ospfLsdbRouterId

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfPacketType	OSPF packet types. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as nullPacket. INTEGER is unknown

ospfLsdbType	The type of the link state advertisement. Each link state type has a separate advertisement format. Note: External link state advertisements are permitted for backward compatibility, but should be displayed in the ospfAsLsdbTable rather than here. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfIfIpAddress	The IP address of this OSPF interface.
ospfAddressLessIf	For the purpose of easing the instancing of addressed and addressless interfaces; this variable takes the value 0 on interfaces with IP addresses and the corresponding value of ifIndex for interfaces having no IP address.
ospfNbrRtrId	A 32-bit integer (represented as a type IpAddress) uniquely identifying the neighboring router in the Autonomous System.
ospfLsdbLsid	The Link State ID is an LS Type Specific field containing either a Router ID or an IP address; it identifies the piece of the routing domain that is being described by the advertisement.
ospfLsdbRouterId	The 32-bit number that uniquely identifies the originating router in the Autonomous System.
ospfNbrAddressLessIndex	On an interface having an IP address, zero. On addressless interfaces, the corresponding value of ifIndex in the Internet Standard MIB. On row creation, this can be derived from the instance.
ospfNbrIpAddr	The IP address that this neighbor is using in its IP source address. Note that, on addressless links, this will not be 0.0.0.0 but the address of another of the neighbor's interfaces.

Go Top

SECTION 7.14

Trap: ospfVirtIfAuthFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfVirtualInterfaceAuthenticationFailure	Trap	Alarm	No	Minor	$NodeDisplayName -- OSPF virtual interface area $ospfVirtIfAreaId, neighbor $ospfVirtIfNeighbor received an OSPF packet of type $ospfPacketType with a configuration error of type $ospfConfigErrorType.	OspfVirtualInterfaceAuthenticationFailure	IP-RAN

Description:

```
An ospfVirtIfAuthFailure trap signifies that a            packet has been received on a virtual interface
from a router whose authentication key or
authentication type conflicts with this router's
authentication key or authentication type.
```

Default Message:

$NodeDisplayName - OSPF virtual interface area $ospfVirtIfAreaId, neighbor $ospfVirtIfNeighbor received an OSPF packet of type $ospfPacketType with a configuration error of type $ospfConfigErrorType.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfConfigErrorType	Potential types of configuration conflicts. Used by the ospfConfigError and ospfConfigVirtError traps. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as noError. INTEGER is unknown
ospfPacketType	OSPF packet types. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as nullPacket. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfVirtIfAreaId	The transit area that the virtual link traverses. By definition, this is not 0.0.0.0.
ospfVirtIfNeighbor	The Router ID of the virtual neighbor.

Go Top

SECTION 7.15

Trap: ospfVirtIfConfigError

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfVirtualInterfaceConfigError	Trap	Alarm	No	Minor	$NodeDisplayName -- OSPF virtual interface area $ospfVirtIfAreaId, neighbor $ospfVirtIfNeighbor received an OSPF packet of type $ospfPacketType with a configuration error of type $ospfConfigErrorType.	OspfVirtualInterfaceConfigError	IP-RAN

Description:

```
An ospfVirtIfConfigError trap signifies that a            packet has been received on a virtual interface
from a router whose configuration parameters
conflict with this router's configuration
parameters.  Note that the event optionMismatch
should cause a trap only if it prevents an
adjacency from forming.
```

Default Message:

$NodeDisplayName - OSPF virtual interface area $ospfVirtIfAreaId, neighbor $ospfVirtIfNeighbor received an OSPF packet of type $ospfPacketType with a configuration error of type $ospfConfigErrorType.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfConfigErrorType	Potential types of configuration conflicts. Used by the ospfConfigError and ospfConfigVirtError traps. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as noError. INTEGER is unknown
ospfPacketType	OSPF packet types. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as nullPacket. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfVirtIfAreaId	The transit area that the virtual link traverses. By definition, this is not 0.0.0.0.
ospfVirtIfNeighbor	The Router ID of the virtual neighbor.

Go Top

SECTION 7.16

Trap: ospfVirtIfRxBadPacket

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfVirtualBadPacketReceived	Trap	Alarm	No	Warning	$NodeDisplayName -- OSPF virtual interface area $ospfVirtIfAreaId, neighbor $ospfVirtIfNeighbor received an OSPF packet of type $ospfPacketType that cannot be parsed.	OspfVirtualBadPacketReceived	IP-RAN

Description:

```
An ospfVirtIfRxBadPacket trap signifies that an OSPF             packet has been received on a virtual interface
that cannot be parsed.
```

Default Message:

$NodeDisplayName - OSPF virtual interface area $ospfVirtIfAreaId, neighbor $ospfVirtIfNeighbor received an OSPF packet of type $ospfPacketType that cannot be parsed.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfPacketType	OSPF packet types. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as nullPacket.

	INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfVirtIfAreaId	The transit area that the virtual link traverses. By definition, this is not 0.0.0.0.
ospfVirtIfNeighbor	The Router ID of the virtual neighbor.

Go Top

SECTION 7.17

Trap: ospfVirtIfStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfVirtualInterfaceState	Trap	Alarm	Yes	Major	$NodeDisplayName -- OSPF virtual interface Area: $ospfVirtIfAreaId, Neighbor: $ospfVirtIfNeighbor changed state to down.	OspfVirtualInterfaceState	IP-RAN
OspfVirtualInterfaceState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF virtual interface Area: $ospfVirtIfAreaId, Neighbor: $ospfVirtIfNeighbor changed state to point-to-point.	OspfVirtualInterfaceState	IP-RAN
OspfVirtualInterfaceState	Poll	Alarm	Yes	Major	$NodeDisplayName - OSPF virtual interface Area: $ospfVirtIfAreaId, Neighbor: $ospfVirtIfNeighbor changed state to down.	OspfVirtualInterfaceState	IP-RAN
OspfVirtualInterfaceState	Poll	Alarm	Yes	Normal	$NodeDisplayName - OSPF virtual interface Area: $ospfVirtIfAreaId, Neighbor: $ospfVirtIfNeighbor changed state to point-to-point.	OspfVirtualInterfaceState	IP-RAN

Description:

```
An ospfVirtIfStateChange trap signifies that there            has been a change in the state of an OSPF virtual
interface.
This trap should be generated when the interface
state regresses (e.g., goes from Point-to-Point to Down)
or progresses to a terminal state
(i.e., Point-to-Point).
```

Default Message:

$NodeDisplayName - OSPF virtual interface Area: $ospfVirtIfAreaId, Neighbor: $ospfVirtIfNeighbor changed state to down/point-point.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfVirtIfState	OSPF virtual interface states. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfVirtIfAreaId	The transit area that the virtual link traverses. By definition, this is not 0.0.0.0.

ospfVirtIfNeighbor	The Router ID of the virtual neighbor.

Go Top

SECTION 7.18

Trap: ospfVirtIfTxRetransmit

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfVirtualRetransmit	Trap	Alarm	No	Warning	$NodeDisplayName -- an OSPF packet of type $ospfPacketType has been retransmitted on an OSPF virtual interface area $ospfVirtIfAreaId, neighbor $ospfVirtIfNeighbor. Link state DB entry: Type: $ospfLsdbType, LsId: $ospfLsdbLsid, RouterId: $ospfLsdbRouterId	OspfVirtualRetransmit	IP-RAN

Description:

```
An ospfVirtIfTxRetransmit trap signifies than an            OSPF packet has been retransmitted on a virtual
interface.  All packets that may be retransmitted
are associated with an LSDB entry.  The LS
type, LS ID, and Router ID are used to identify
the LSDB entry.
```

Default Message:

$NodeDisplayName - an OSPF packet of type $ospfPacketType has been retransmitted on an OSPF virtual interface area $ospfVirtIfAreaId, neighbor $ospfVirtIfNeighbor. Link state DB entry: Type: $ospfLsdbType, LsId: $ospfLsdbLsid, RouterId: $ospfLsdbRouterId

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfPacketType	OSPF packet types. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as nullPacket. INTEGER is unknown
ospfLsdbType	The type of the link state advertisement. Each link state type has a separate advertisement format. Note: External link state advertisements are permitted for backward compatibility, but should be displayed in the ospfAsLsdbTable rather than here. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfVirtIfAreaId	The transit area that the virtual link traverses. By definition, this is not 0.0.0.0.
ospfVirtIfNeighbor	The Router ID of the virtual neighbor.
ospfLsdbLsid	The Link State ID is an LS Type Specific field

	containing either a Router ID or an IP address; it identifies the piece of the routing domain that is being described by the advertisement.
ospfLsdbRouterId	The 32-bit number that uniquely identifies the originating router in the Autonomous System.
ospfLsdbAreaId	The 32-bit identifier of the area from which the LSA was received.

Go Top

SECTION 7.19

Trap: ospfVirtNbrRestartHelperStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfVirtualNeighborRestartHelperState	Trap	Alarm	Yes	Informational	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea, Router ID: $ospfVirtNbrRtrId restart status changed. Status: helping, Age: $ospfVirtNbrRestartHelperAge, Exit Reason: $ospfVirtNbrRestartHelperExitReason.	OspfVirtualNeighborRestartHelperState	IP-RAN
OspfVirtualNeighborRestartHelperState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea, Router ID: $ospfVirtNbrRtrId restart status changed. Status: not helping, Age: $ospfVirtNbrRestartHelperAge, Exit Reason: $ospfVirtNbrRestartHelperExitReason.	OspfVirtualNeighborRestartHelperState	IP-RAN
OspfVirtualNeighborRestartHelperState	Poll	Alarm	Yes	Informational	$NodeDisplayName - OSPF virtual neighbor area $ospfVirtNbrArea, Router ID: $ospfVirtNbrRtrId restart status changed. Status: helping.	OspfVirtualNeighborRestartHelperState	IP-RAN
OspfVirtualNeighborRestartHelperState	Poll	Alarm	Yes	Normal	$NodeDisplayName . OSPF virtual neighbor area $ospfVirtNbrArea, Router ID: $ospfVirtNbrRtrId restart status changed. Status: not helping.	OspfVirtualNeighborRestartHelperState	IP-RAN

Description:

```
An ospfVirtNbrRestartHelperStatusChange trap signifies            that there has been a change in the graceful restart
helper state for the virtual neighbor.  This trap should
be generated when the virtual neighbor restart helper
status transitions for a virtual neighbor.
```

Default Message:

$NodeDisplayName - OSPF virtual neighbor area $ospfVirtNbrArea, Router ID: $ospfVirtNbrRtrId restart status changed. Status: helping/not helping, Age: $ospfVirtNbrRestartHelperAge, Exit Reason: $ospfVirtNbrRestartHelperExitReason.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfVirtNbrRestartHelperStatus	Indicates whether the router is acting as a graceful restart helper for the neighbor. INTEGER is unknown
ospfVirtNbrRestartHelperExitReason	Describes the outcome of the last attempt at acting as a graceful restart helper for the neighbor. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System.

	By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfVirtNbrArea	The Transit Area Identifier.
ospfVirtNbrRtrId	A 32-bit integer uniquely identifying the neighboring router in the Autonomous System.
ospfVirtNbrRestartHelperAge	Remaining time in current OSPF graceful restart interval, if the router is acting as a restart helper for the neighbor.

Go Top

SECTION 7.20

Trap: ospfVirtNbrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfVirtualNeighborState	Trap	Alarm	Yes	Major	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to down.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to attempt.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to init.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to two-way.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to exchangeStart.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to exchange.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Trap	Event	Yes	Informational	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to loading.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to full.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Poll	Alarm	Yes	Major	$NodeDisplayName . OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to down.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName . OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to attempt.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName . OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to init.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Poll	Alarm	Yes	Normal	$NodeDisplayName . OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to two-way.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName . OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to exchangeStart.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName . OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to exchange.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Poll	Alarm	Yes	Informational	$NodeDisplayName . OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to loading.	OspfVirtualNeighborState	IP-RAN
OspfVirtualNeighborState	Poll	Alarm	Yes	Normal	$NodeDisplayName . OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to full.	OspfVirtualNeighborState	IP-RAN

Description:

```
An ospfVirtNbrStateChange trap signifies that there            has been a change in the state of an OSPF virtual
neighbor.  This trap should be generated
when the neighbor state regresses (e.g., goes
from Attempt or Full to 1-Way or Down) or
progresses to a terminal state (e.g., Full).
```

Default Message:

$NodeDisplayName -- OSPF virtual neighbor area $ospfVirtNbrArea on $ospfVirtNbrRtrId changed state to $ospfVirtNbrState.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfVirtNbrState	The state of the virtual neighbor relationship. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfVirtNbrArea	The Transit Area Identifier.
ospfVirtNbrRtrId	A 32-bit integer uniquely identifying the neighboring router in the Autonomous System.

Go Top

SECTION 7.21

Trap: entSensorThresholdNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EntitySensorThresholdState	Trap	Event	Yes	Informational	$NodeDisplayName -- Entity sensor reports the value $entSensorValue crossed the threshold $entSensorThresholdValue.	EntitySensorThresholdState	IP-RAN
EntitySensorThresholdState	Poll	Alarm	Yes	Warning	$NodeDisplayName -- $entPhysicalDescr reports the value $entSensorValue $entSensorType which is $entSensorThresholdRelation the threshold $entSensorThresholdValue $entSensorType. Data scale is $entSensorScale.	EntitySensorThresholdState	IP-RAN
EntitySensorThresholdState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- $entPhysicalDescr reports the value $entSensorValue $entSensorType which is $entSensorThresholdRelation the threshold $entSensorThresholdValue $entSensorType. Data scale is $entSensorScale.	EntitySensorThresholdState	IP-RAN
EntitySensorThresholdState	Poll	Alarm	Yes	Major	$NodeDisplayName -- $entPhysicalDescr reports the value $entSensorValue $entSensorType which is $entSensorThresholdRelation the threshold $entSensorThresholdValue $entSensorType. Data scale is $entSensorScale.	EntitySensorThresholdState	IP-RAN
EntitySensorThresholdState	Poll	Alarm	Yes	Critical	$NodeDisplayName -- $entPhysicalDescr reports the value $entSensorValue $entSensorType which is $entSensorThresholdRelation the threshold $entSensorThresholdValue $entSensorType. Data scale is $entSensorScale.	EntitySensorThresholdState	IP-RAN
EntitySensorThresholdState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- $entPhysicalDescr reports the value $entSensorValue $entSensorType which is within the normal range. Data scale is $entSensorScale.	EntitySensorThresholdState	IP-RAN

Description:

```
The sensor value crossed the threshold         listed in entSensorThresholdTable.
This notification is generated once each time
the sensor value crosses the threshold.

The agent implementation guarantees prompt, timely
evaluation of threshold and generation of this
notification.
```

Default Message:

$NodeDisplayName - Entity sensor reports the value $entSensorValue crossed the threshold $entSensorThresholdValue.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
entSensorThresholdValue	This variable indicates the value of the threshold. To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision. However, you can directly compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge.
entSensorValue	This variable reports the most recent measurement seen by the sensor. To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision. However, you can compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge.
entPhysicalIndex	The index for this entry.
entSensorThresholdIndex	An index that uniquely identifies an entry in the entSensorThresholdTable. This index permits the same sensor to have several different thresholds.

Go Top

SECTION 7.22

Trap: ciscoIpMRouteMissingHeartBeats

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPMRouteHeartBeat	Trap	Alarm	No	Warning	$NodeDisplayName - Multicast router failed to receive the configured heartbeat packets, heartbeat packet source : $ciscoIpMRouteHeartBeatSourceAddr, heartbeat interval : $ciscoIpMRouteHeartBeatInterval . hearbeat Window Size : $ciscoIpMRouteHeartBeatWindowSize, Hearbeat Count : $ciscoIpMRouteHeartBeatCount	IPMRouteHeartBeat	IP-RAN

Description:

```
A ciscoIpMRouteMissingHeartBeat is sent if a multicast router        with this feature enabled failed to receive configured number
of heartbeat packets from heartbeat sources within a
configured time interval.
```

Default Message:

$NodeDisplayName - Multicast router failed to receive the configured heartbeat packets, heartbeat packet source : $ciscoIpMRouteHeartBeatSourceAddr, heartbeat interval : $ciscoIpMRouteHeartBeatInterval . hearbeat Window Size : $ciscoIpMRouteHeartBeatWindowSize, Hearbeat Count : $ciscoIpMRouteHeartBeatCount.

Message Substitution Variables:

Common	Substitution variables common to all traps.

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ciscoIpMRouteHeartBeatSourceAddr	Source address of the last multicast heartbeat packet received.
ciscoIpMRouteHeartBeatInterval	Number of seconds in which a Cisco multicast router expects a valid heartBeat packet from a source. This value must be a multiple of 10.
ciscoIpMRouteHeartBeatWindowSize	Number of ciscoIpMRouteHeartBeatInterval intervals a Cisco multicast router waits before checking if expected number of heartbeat packets are received or not.
ciscoIpMRouteHeartBeatCount	Number of time intervals where multicast packets were received in the last ciscoIpMRouteHeartBeatWindowSize intervals.
ciscoIpMRouteHeartBeatGroupAddr	Multicast group address used to receive heartbeat packets.

Go Top

SECTION 7.23

Trap: ciscoMvpnMvrfChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MulticastVPNMvrfChange	Trap	Event	No	Informational	$NodeDisplayName - A new MVRF has been added in the device.	MulticastVPNMvrfChange	IP-RAN
MulticastVPNMvrfChange	Trap	Alarm	No	Warning	$NodeDisplayName - An MVRF entry has been deleted in the device.	MulticastVPNMvrfChange	IP-RAN
MulticastVPNMvrfChange	Trap	Event	No	Informational	$NodeDisplayName - A MVRF Mdt config entry has been modified in the device.	MulticastVPNMvrfChange	IP-RAN
MulticastVPNMvrfChange	Trap	Event	No	Informational	$NodeDisplayName - A MVRF data Mdt config entry has been modified in the device.	MulticastVPNMvrfChange	IP-RAN

Description:

```
A ciscoMvpnMvrfChange notification signifies a change about
the MVRF, deletion of the MVRF or an update on the default
or data MDT configuration of the MVRF. The change event
is indicated by ciscoMvpnGenOperStatusChange embedded in
the notification. The user can then query
ciscoMvpnGenericTable, ciscoMvpnMdtDefaultTable and/or
ciscoMvpnMdtDataTable to get the details of the change as
necessary.
Note: Since the creation of a MVRF is often followed by
configuration of default and data MDT groups for the MVRF,
more than one (three at most) notifications for a MVRF may
be generated serially, and it is really not necessary to
generate all three of them. An agent may choose to generate a
notification for the last event only, that is for data MDT
configuration.
Similarly, deletion of default or data MDT configuration on a
MVRF happens before a MVRF is deleted, it is recommended
that the agent send the notification for MVRF deletion
event only.
```

```
a MVRF in the device. The change event can be creation of
```

Default Message:

$NodeDisplayName - A new MVRF has been added in the device.
$NodeDisplayName - An MVRF entry has been deleted in the device.
$NodeDisplayName - A MVRF Mdt config entry has been modified in the device.
$NodeDisplayName - A MVRF data Mdt config entry has been modified in the device.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ciscoMvpnGenOperStatusChange	This object describes the last operational change that happened for the given MVRF.

	createdMvrf - indicates that the MVRF was created in the device. deletedMvrf - indicates that the MVRF was deleted from the device. A row in this table will never have ciscoMvpnGenOperStatusChange equal to deletedMvrf(2), because in that case the row itself will be deleted from the table. This value for ciscoMvpnGenOperStatusChange is defined mainly for use in ciscoMvpnMvrfChange notification. modifiedMvrfDefMdtConfig - indicates that the default MDT group for the MVRF was configured, deleted or changed. modifiedMvrfDataMdtConfig - indicates that the data MDT group range or a associated variable (like the threshold) for the MVRF was configured, deleted or changed. INTEGER is unknown
mplsVpnVrfName	The human-readable name of this VPN. This MAY be equivalent to the RFC2685 VPN-ID.

Go Top

SECTION 7.24

Trap: ciscoPimInterfaceDown

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PimInterfaceState	Trap	Alarm	Yes	Critical	$NodeDisplayName - The PIM Interface $IfName is down.	PimInterfaceState	IP-RAN
PimInterfaceState	Trap	Alarm	Yes	Normal	$NodeDisplayName - The PIM Interface $IfName is active.	PimInterfaceState	IP-RAN

Description:

```
A ciscoPimInterfaceDown notification signifies the loss           of a PIM interface. This notification should be generated
whenever an entry is about to be deleted from the
PimInterfaceTable.
pimInterfaceStatus identifies the interface which
was involved in the generation of this notification.
```

Default Message:

$NodeDisplayName - The PIM Interface is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
IfAlias	The interface alias.
IfName	The interface name.
pimInterfaceStatus	The status of this entry. Creating the entry enables PIM on the interface; destroying the entry disables PIM on the interface. RowStatus is unknown
pimInterfaceIfIndex	The ifIndex value of this PIM interface.

Go Top

SECTION 7.25

Trap: ciscoPimInvalidJoinPrune

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PIMInvalidJoinPrune	Trap	Alarm	No	Warning	$NodeDisplayName - An invalid join or prune message is received. Last Error origin : $cpimLastErrorOrigin, Last Error Group : $cpimLastErrorGroup, Last Error RP : $cpimLastErrorRP. Number of Join or Prune messages received is $cpimInvalidJoinPruneMsgsRcvd.	PIMInvalidJoinPrune	IP-RAN

Description:

```
A ciscoPimInvalidJoinPrune notification signifies the           receipt of an invalid join/prune message.

This notification is generated whenever the
cpimInvalidJoinPruneMsgsRcvd counter is incremented.
cpimLastErrorOrigin, cpimLastErrorGroup, and
cpimLastErrorRP should signify the source address, group
address and the RP address in the invalid join/prune
packet.
```

Default Message:

$NodeDisplayName - An invalid join or prune message is received. Last Error origin : $cpimLastErrorOrigin, Last Error Group : $cpimLastErrorGroup, Last Error RP : $cpimLastErrorRP. Number of Join or Prune messages received is $cpimInvalidJoinPruneMsgsRcvd.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cpimLastErrorOriginType	Represents the type of address stored in cpimLastErrorOrigin. The value of this object is irrelevant if the value of cpimLastErrorType is none(1). A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In

	particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cpimLastErrorGroupType	Represents the type of address stored in cpimLastErrorGroup. The value of this object is unknown(0) if there is a problem in the packet received from the DR. The value of this object is irrelevant if the value of cpimLastErrorType is none(1). A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cpimLastErrorRPType	Represents the type of address stored in cpimLastErrorRP. The value of this object is irrelevant if the value of cpimLastErrorType is none(1). A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions.

	It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cpimLastErrorOrigin	This object represents the Network Layer Address of the source that originated the last invalid packet. The type of address stored depends on the value in cpimLastErrorOriginType. The value of this object represents the Network Layer Address of the Designated Router (DR) whenever the value of cpimLastErrorGroup is a zero-length address, for eg. when encapsulated IP header is malformed. The value of this object is irrelevant if the value of cpimLastErrorType is none(1).
cpimLastErrorGroup	The IP multicast group address to which the last invalid packet was addressed. The type of address stored depends on the value in cpimLastErrorGroupType. The value of this object is a zero-length InetAddress if there is a problem in the packet received from the DR, for eg. a malformed encapsulated IP header. The value of this object is irrelevant if the value of cpimLastErrorType is none(1).
cpimLastErrorRP	The address of the RP, as per the last invalid packet. The type of address stored depends on the value in cpimLastErrorRPType. The value of this object is irrelevant if the value of cpimLastErrorType is none(1).
cpimInvalidJoinPruneMsgsRcvd	A count of the number of invalid PIM Join/Prune messages received by this device. A PIM Join/Prune message is termed invalid if o the RP specified in the packet is not the RP for the group in question.

Go Top

SECTION 7.26

Trap: ciscoPimInvalidRegister

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PIMInvalidRegister	Trap	Alarm	No	Warning	$NodeDisplayName - An invalid register message is received. Last Error origin : $cpimLastErrorOrigin, Last Error Group : $cpimLastErrorGroup, Last Error RP : $cpimLastErrorRP. Number of Invalid error message received is $cpimInvalidRegisterMsgsRcvd.	PIMInvalidRegister	IP-RAN

Description:

```
A ciscoPimInvalidRegister notification signifies that            an invalid Register message was received by this device.

This notification is generated whenever the
cpimInvalidRegisterMsgsRcvd counter is incremented.
cpimLastErrorOrigin, cpimLastErrorGroup, and
cpimLastErrorRP should signify the source address, group
address and the RP address in the invalid register
packet.
```

Default Message:

$NodeDisplayName - An invalid register message is received. Last Error origin : $cpimLastErrorOrigin, Last Error Group : $cpimLastErrorGroup, Last Error RP : $cpimLastErrorRP. Number of Invalid error message received is $cpimInvalidRegisterMsgsRcvd.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cpimLastErrorOriginType	Represents the type of address stored in cpimLastErrorOrigin. The value of this object is irrelevant if the value of cpimLastErrorType is none(1). A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cpimLastErrorGroupType	Represents the type of address stored in cpimLastErrorGroup. The value of this object is unknown(0) if there is a problem in the packet received from the DR. The value of this object is irrelevant if the value of cpimLastErrorType is none(1). A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention.

	ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cpimLastErrorRPType	Represents the type of address stored in cpimLastErrorRP. The value of this object is irrelevant if the value of cpimLastErrorType is none(1). A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cpimLastErrorOrigin	This object represents the Network Layer Address of the source that originated the last invalid packet. The type of address stored depends on the value in cpimLastErrorOriginType. The value of this object represents the Network Layer Address of the Designated Router (DR) whenever the value of cpimLastErrorGroup is a zero-length address, for eg. when encapsulated IP header is malformed. The value of this object is irrelevant if the value of cpimLastErrorType is none(1).
cpimLastErrorGroup	The IP multicast group address to which the last invalid packet was addressed. The type of address stored

	depends on the value in cpimLastErrorGroupType. The value of this object is a zero-length InetAddress if there is a problem in the packet received from the DR, for eg. a malformed encapsulated IP header. The value of this object is irrelevant if the value of cpimLastErrorType is none(1).
cpimLastErrorRP	The address of the RP, as per the last invalid packet. The type of address stored depends on the value in cpimLastErrorRPType. The value of this object is irrelevant if the value of cpimLastErrorType is none(1).
cpimInvalidRegisterMsgsRcvd	A count of the number of invalid PIM Register messages received by this device. A PIM Register message is termed invalid if o the encapsulated IP header is malformed, o the destination of the PIM Register message is not the RP (Rendezvous Point) for the group in question, o the source/DR (Designated Router) address is not a valid unicast address.

Go Top

SECTION 7.27

Trap: ciscoPimRPMappingChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PIMRPMappingChange	Trap	Event	No	Informational	$NodeDisplayName - A new mapping has been added into the RP Set Table.	PIMRPMappingChange	IP-RAN
PIMRPMappingChange	Trap	Alarm	No	Warning	$NodeDisplayName - A mapping has been deleted from the RP Set Table.	PIMRPMappingChange	IP-RAN
PIMRPMappingChange	Trap	Event	No	Informational	$NodeDisplayName - New mapping entry in the RPSetTable has been modified.	PIMRPMappingChange	IP-RAN
PIMRPMappingChange	Trap	Event	No	Informational	$NodeDisplayName - Old mapping entry in the RPSetTable has been modified.	PIMRPMappingChange	IP-RAN

Description:

```
A ciscoPimRPMappingChange notification signifies a change in the RP Mapping on the device in question. A change in RP
Mapping could be because of addition of new entries to the
RP Mapping cache, deletion of existing entries, or a
modification to an existing mapping. The type of change is
indicated by cpimRPMappingChangeType. pimRPSetHoldTime
is used to identify the row in the pimRPSetTable that is
responsible for the generation of this notification.
In case of modification to existing entries, a
notification should be generated once before the
modification (with cpimRPMappingChangeType set to
modifiedOldMapping) and once after modification (with
cpimRPMappingChangeType set to modifiedNewMapping).
NOTE: A high frequency of RP Mapping change could result
in a large number of ciscoPimRPMappingChange notifications
being generated. Hence, in environments where the
possibility of a high frequency of RP Mapping change
exists, enable this notification with utmost care.
```

Default Message:

$NodeDisplayName - A new mapping has been added into the RP Set Table.
$NodeDisplayName - A mapping has been deleted from the RP Set Table.
$NodeDisplayName - New mapping entry in the RPSetTable has been modified.
$NodeDisplayName - Old mapping entry in the RPSetTable has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

cpimRPMappingChangeType	Describes the operation that resulted in generation of cpimRPMappingChange notification. o newMapping, as the name suggests indicates that a new mapping has been added into the pimRPSetTable, o deletedMapping indicates that a mapping has been deleted from the pimRPSetTable, and, o modifiedXXXMapping indicates that an RP mapping (which already existed in the table) has been modified. The two modifications types i.e. modifiedOldMapping and modifiedNewMapping, are defined to differentiate the notification generated before modification from that generated after modification. INTEGER is unknown
pimRPSetHoldTime	The holdtime of a Candidate-RP. If the local router is not the BSR, this value is 0.
pimRPSetComponent	A number uniquely identifying the component. Each protocol instance connected to a separate domain should have a different index value.
pimRPSetAddress	The IP address of the Candidate-RP.
pimRPSetGroupMask	The multicast group address mask which, when combined with pimRPSetGroupAddress, gives the group prefix for which this entry contains information about the Candidate-RP.
pimRPSetGroupAddress	The IP multicast group address which, when combined with pimRPSetGroupMask, gives the group prefix for which this entry contains information about the Candidate-RP.

Go Top

SECTION 7.28

Trap: pimNeighborLoss

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PIMNeighborState	Trap	Alarm	No	Major	$NodeDisplayName - The Router has lost its neighbors.	PIMNeighborState	IP-RAN

Description:

```
A pimNeighborLoss trap signifies the loss of an adjacency           with a neighbor.  This trap should be generated when the
neighbor timer expires, and the router has no other
neighbors on the same interface with a lower IP address than
itself.
```

Default Message:

$NodeDisplayName - The Router has lost its neighbors.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
pimNeighborIfIndex	The value of ifIndex for the interface used to reach this PIM neighbor.
pimNeighborAddress	The IP address of the PIM neighbor for which this entry contains information.

Go Top

SECTION 7.29

Trap: cbgpFsmStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CbgpFsmState	Trap	Alarm	Yes	Minor	$NodeDisplayName - BGP FSM state is changed to idle.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Alarm	Yes	Major	$NodeDisplayName - BGP FSM state is changed to connect.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Alarm	Yes	Major	$NodeDisplayName - BGP FSM state is changed to active.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Event	Yes	Informational	$NodeDisplayName - BGP FSM state is changed to opensent.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Event	Yes	Informational	$NodeDisplayName - BGP FSM state is changed to openconfirm.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Alarm	Yes	Normal	$NodeDisplayName - BGP FSM state is changed to established.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Alarm	Yes	Minor	$NodeDisplayName - BGP FSM state is changed to idle.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Alarm	Yes	Major	$NodeDisplayName - BGP FSM state is changed to connect.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Alarm	Yes	Major	$NodeDisplayName - BGP FSM state is changed to active.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Event	Yes	Informational	$NodeDisplayName - BGP FSM state is changed to opensent.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Event	Yes	Informational	$NodeDisplayName - BGP FSM state is changed to openconfirm.	CbgpFsmState	IP-RAN
CbgpFsmState	Trap	Alarm	Yes	Normal	$NodeDisplayName - BGP FSM state is changed to established.	CbgpFsmState	IP-RAN
CbgpFsmState	Poll	Alarm	Yes	Minor	$NodeDisplayName - BGP FSM state is changed to idle.	CbgpFsmState	IP-RAN
CbgpFsmState	Poll	Alarm	Yes	Major	$NodeDisplayName - BGP FSM state is changed to connect.	CbgpFsmState	IP-RAN
CbgpFsmState	Poll	Alarm	Yes	Major	$NodeDisplayName - BGP FSM state is changed to active.	CbgpFsmState	IP-RAN
CbgpFsmState	Poll	Event	Yes	Informational	$NodeDisplayName - BGP FSM state is changed to opensent.	CbgpFsmState	IP-RAN
CbgpFsmState	Poll	Event	Yes	Informational	$NodeDisplayName - BGP FSM state is changed to openconfirm.	CbgpFsmState	IP-RAN
CbgpFsmState	Poll	Alarm	Yes	Normal	$NodeDisplayName - BGP FSM state is changed to established.	CbgpFsmState	IP-RAN

Description:

```
The BGP cbgpFsmStateChange notification is generated for every BGP FSM state change. The bgpPeerRemoteAddr
value is attached to the notification object ID.
```

Default Message:

$NodeDisplayName - BGP FSM state is changed to $bgpPeerState.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
bgpPeerState	The BGP peer connection state. INTEGER is unknown
cbgpPeerPrevState	The BGP peer connection previous state. INTEGER is unknown
bgpPeerLastError	The last error code and subcode seen by this peer on this connection. If no error has occurred, this field is zero. Otherwise, the first byte of this two byte OCTET STRING contains the error code, and the second byte contains the subcode.
cbgpPeerLastErrorTxt	Implementation specific error description for bgpPeerLastErrorReceived.
bgpPeerRemoteAddr	The remote IP address of this entry's BGP peer.

Go Top

SECTION 7.30

Trap: cbgpPrefixThresholdClear

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

CbgpPrefixThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName - Prefix count has dropped below $cbgpPeerPrefixClearThreshold.	CbgpPrefixThreshold	IP-RAN
CbgpPrefixThreshold	Trap	Alarm	Yes	Warning	$NodeDisplayName - Prefix threshold count reached to $cbgpPeerPrefixThreshold.	CbgpPrefixThreshold	IP-RAN

Description:

```
The cbgpPrefixThresholdClear notification is generated when prefix count drops below the configured
clear threshold on a session for an address family once cbgpPrefixThresholdExceeded is generated. This won't
be generated if the peer session goes down after the generation of cbgpPrefixThresholdExceeded.
The bgpPeerRemoteAddr, cbgpPeerAddrFamilyAfi and cbgpPeerAddrFamilySafi values are attached to the
notification object ID.
```

Default Message:

Prefix count has dropped below $cbgpPeerPrefixClearThreshold.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cbgpPeerPrefixAdminLimit	Max number of route prefixes accepted for an address family on this connection.
cbgpPeerPrefixClearThreshold	Prefix threshold value (%) for an address family on this connection at which SNMP clear notification is generated if prefix threshold notification is already generated.
cbgpPeerAddrFamilyAfi	The AFI index of the entry. An implementation is only required to support IPv4 unicast and VPNv4 (Value - 1) address families.
cbgpPeerAddrFamilySafi	The SAFI index of the entry. An implementation is only required to support IPv4 unicast(Value - 1) and VPNv4(Value - 128) address families.
bgpPeerRemoteAddr	The remote IP address of this entry's BGP peer.

Go Top

SECTION 7.31

Trap: ciscoBfdSessDown

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BFDSessionState	Trap	Alarm	Yes	Critical	BFDSession of $NodeDisplayName changed state from Active to Down	BFDSessionState	IP-RAN
BFDSessionState	Trap	Alarm	Yes	Normal	BFDSession of $NodeDisplayName changed state from Down to Active	BFDSessionState	IP-RAN

Description:

```
This notification is generated when the        ciscoBfdSessState object for one or more contiguous
entries in ciscoBfdSessTable are about to enter the down(2)
or adminDown(1) states from some other state. The included
values of ciscoBfdSessDiag MUST both be set equal to this
new state (i.e: down(2) or adminDown(1)).  The two instances
of ciscoBfdSessDiag in this notification indicate the range
of indexes that are affected.  Note that all the indexes
of the two ends of the range can be derived from the
instance identifiers of these two objects.  For
cases where a contiguous range of sessions
have transitioned into the down(2) or adminDown(1) states
at roughly the same time, the device SHOULD issue a single
notification for each range of contiguous indexes in
an effort to minimize the emission of a large number
of notifications.  If a notification has to be
issued for just a single ciscoBfdSessEntry, then
the instance identifier (and values) of the two
ciscoBfdSessDiag objects MUST be the identical.
```

Default Message:

BFDSession of $NodeDisplayName changed state from Active to Down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ciscoBfdSessDiag	A diagnostic code specifying the local system's reason for the last transition of the session from up(1) to some other state. A common BFD diagnostic code.
ciscoBfdSessDiag	A diagnostic code specifying the local system's reason for the last transition of the session from up(1) to some other state. A common BFD diagnostic code.
ciscoBfdSessIndex	This object contains an index used to represent a unique BFD session on this device.

Go Top

SECTION 7.32

Status: EntitySensorState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EntitySensorState	Poll	Alarm	Yes	Major	$NodeDisplayName - Entity sensor $entPhysicalDescr is nonoperational	EntitySensorState	IP-RAN
EntitySensorState	Poll	Alarm	Yes	Normal	$NodeDisplayName - Entity sensor $entPhysicalDescr is ok	EntitySensorState	IP-RAN

Description:

```
This status alarm is issued based        on the value of the entSensorStatus
listed in entSensorValueTable.
```

Default Message:

$NodeDisplayName - Entity sensor $entPhysicalDescr is $entSensorStatus

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
entPhysicalDescr	A textual description of physical entity. This object should contain a string which identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.
entSensorStatus	This variable indicates the present operational status of the sensor.
entPhysicalIndex	The index for this entry.

Go Top

SECTION 7.33

Status: CardStateAdded and CardStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

CardState	Poll	Alarm	Yes	Normal	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName added in state Active/ActiveReason.	CardState	IP-RAN
CardState	Poll	Event	Yes	Warning	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName added in state Warning/WarningReason.	CardState	IP-RAN
CardState	Poll	Event	Yes	Warning	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName added in state Unknown/UnknownReason.	CardState	IP-RAN
CardState	Poll	Alarm	Yes	Critical	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName added in state Failed/FailedReason.	CardState	IP-RAN
CardState	Poll	Event	Yes	Informational	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName added in state $CardState/$CardStateReason.	CardState	IP-RAN
CardState	Poll	Alarm	Yes	Normal	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName changed state from $CardLastState to Active/ActiveReason.	CardState	IP-RAN
CardState	Poll	Event	Yes	Warning	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName changed state from $CardLastState to Warning/WarningReason.	CardState	IP-RAN
CardState	Poll	Alarm	Yes	Critical	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName changed state from $CardLastState to Failed/FailedReason.	CardState	IP-RAN
CardState	Poll	Event	Yes	Warning	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName changed state from $CardLastState to Unknown/UnknownReason.	CardState	IP-RAN
CardState	Poll	Event	Yes	Informational	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName changed state from $CardLastState to $CardState/$CardStateReason.	CardState	IP-RAN

Description:

The CardStateAdded and CardStateChanged status events provide information when a Card object is added to the MWTM object model or when MWTM detects that the state of a Card has changed. The value of CardState indicates the new
state. Possible values of CardState include:

- Active - Traffic may flow over this Card.
- Unknown - The attempt to determine the state of the Card failed.
- Warning - The Card is Active however some underlying interface of this Card is not fully functional.
- NotPresent - The Card is configured but not physically present in the chassis.
- Failed - The Card is not functional.
- Deleted - The Card has been deleted from the object database.

Default Message:

- Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName added in state $CardState/$CardStateReason.
- Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName changed state from $CardLastState to $CardState/$CardStateReason.

Message Substitution Variables:

Nodeof the Card.

Substitution variables for Node related data.	
CardDisplayName	The name of the Card.
CardSlotNumber	The slot number of the Card.
CardState	The current state of the Card.
CardStateReason	The current state reason of the Card.
CardLastState	The previous state of the Card.

Operational Information:

See also:

Go Top

SECTION 7.34

Status: RanBackhaulStateAdded and RanBackhaulStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RanBackhaulState	Poll	Alarm	Yes	Normal	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName added in state Active/ActiveReason.	RanBackhaulState	IP-RAN
RanBackhaulState	Poll	Alarm	Yes	Warning	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName added in state Warning/WarningReason.	RanBackhaulState	IP-RAN
RanBackhaulState	Poll	Event	Yes	Warning	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName added in state	RanBackhaulState	IP-RAN

					Unknown/UnknownReason.		
RanBackhaulState	Poll	Alarm	Yes	Critical	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName added in state Failed/FailedReason.	RanBackhaulState	IP-RAN
RanBackhaulState	Poll	Event	Yes	Informational	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName added in state $RanBackhaulState/$RanBackhaulStateReason.	RanBackhaulState	IP-RAN
RanBackhaulState	Poll	Alarm	Yes	Normal	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName changed state from $RanBackhaulLastState to Active/ActiveReason.	RanBackhaulState	IP-RAN
RanBackhaulState	Poll	Alarm	Yes	Warning	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName changed state from $RanBackhaulLastState to Warning/WarningReason.	RanBackhaulState	IP-RAN
RanBackhaulState	Poll	Event	Yes	Warning	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName changed state from $RanBackhaulLastState to Unknown/UnknownReason.	RanBackhaulState	IP-RAN
RanBackhaulState	Poll	Alarm	Yes	Critical	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName changed state from $RanBackhaulLastState to Failed/FailedReason.	RanBackhaulState	IP-RAN
RanBackhaulState	Poll	Event	Yes	Informational	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName changed state from $RanBackhaulLastState to $RanBackhaulState/$RanBackhaulStateReason.	RanBackhaulState	IP-RAN

Description:

The RanBackhaulStateAdded and RanBackhaulStateChanged status eventsprovide information when a RanBackhaul object is added to the MWTM object model or when MWTM detects that the state of a RanBackhaul has changed. The value of RanBackhaulState indicates the new state.
Possible values of RanBackhaulState include:

- Active - Traffic may flow over this RanBackhaul.
- Unknown - The attempt to determine the state of the RanBackhaul failed.
- Warning - The RanBackhaul is Active however some underlying interface of this RanBackhaul is not fully functional.
- Failed - All underlying interfaces are not functional.
- Deleted - The RanBackhaul has been deleted from the object database.

Default Message:

- RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName added in state $RanBackhaulState/$RanBackhaulStateReason.
- RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName changed state from $RanBackhaulLastState to $RanBackhaulState/$RanBackhaulStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.
RanBackhaulDisplayName	The name of the RanBackhaul.
RanBackhaulState	The current state of the RanBackhaul.
RanBackhaulStateReason	The current state reason of of the RanBackhaul.
RanBackhaulLastState	The previous state of the RanBackhaul.

Operational Information:

See also:

Go Top

SECTION 7.35

Status: RanBackhaulRcvdUtilChanged and RanBackhaulSentUtilChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RanBackhaulRcvdUtil	Poll	Alarm	Yes	Normal	RanBackhaul $BackhaulDisplayName receive utilization percentage has changed to $BackhaulUtilization, new state is Acceptable.	RanBackhaulRcvdUtil	IP-RAN

RanBackhaulRcvdUtil	Poll	Alarm	Yes	Warning	RanBackhaul $BackhaulDisplayName receive utilization percentage has changed to $BackhaulUtilization, new state is Warning.	RanBackhaulRcvdUtil	IP-RAN
RanBackhaulRcvdUtil	Poll	Alarm	Yes	Critical	RanBackhaul $BackhaulDisplayName receive utilization percentage has changed to $BackhaulUtilization, new state is Overloaded.	RanBackhaulRcvdUtil	IP-RAN

Description:

The RanBackhaulRcvdUtilChanged and RanBackhaulSentUtilChanged events notify network management applications of changes in backhaul link utilization. The utilization state indicates either Acceptable, Warning or Overloaded :

- Acceptable - traffic for a specified direction is at acceptable level.
- Warning - traffic for a specified direction is above acceptable level but below the overloaded level.
- Overloaded - traffic for a specified direction has reached or exceeds overloaded level.

Default Message:

- RanBackhaul $BackhaulDisplayName receive utilization percentage has changed to $BackhaulUtilization, new state is $BackhaulUtilState.
- RanBackhaul $BackhaulDisplayName sent utilization percentage has changed to $BackhaulUtilization, new state is $BackhaulUtilState.

Message Substitution Variables:

Node

Substitution variables for Node related data. This is only valid for real backhaul objects.
Virtual objects will have no associated node data.

BackhaulDisplayName	The name of the backhaul. For a real backhaul this will be of the form 'nodename/backhaulname'. For virtual backhauls there will be no node indicator.
BackhaulUtilState	The current state either Acceptable, Warning or Overloaded.
BackhaulUtilization	The average receive/transmit utilization of link over the last second.

Go Top

SECTION 7.36

Status: RanBackhaulRcvdUtilChanged and RanBackhaulSentUtilChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RanBackhaulSentUtil	Poll	Alarm	Yes	Normal	RanBackhaul $BackhaulDisplayName sent utilization percentage has changed to $BackhaulUtilization, new state is Acceptable.	RanBackhaulSentUtil	IP-RAN
RanBackhaulSentUtil	Poll	Alarm	Yes	Warning	RanBackhaul $BackhaulDisplayName sent utilization percentage has changed to $BackhaulUtilization, new state is Warning.	RanBackhaulSentUtil	IP-RAN
RanBackhaulSentUtil	Poll	Alarm	Yes	Critical	RanBackhaul $BackhaulDisplayName sent utilization percentage has changed to $BackhaulUtilization, new state is Overloaded.	RanBackhaulSentUtil	IP-RAN

Description:

The RanBackhaulRcvdUtilChanged and RanBackhaulSentUtilChanged events notify network management applications of changes in backhaul link utilization. The utilization state indicates either Acceptable, Warning or Overloaded :

- Acceptable - traffic for a specified direction is at acceptable level.
- Warning - traffic for a specified direction is above acceptable level but below the overloaded level.
- Overloaded - traffic for a specified direction has reached or exceeds overloaded level.

Default Message:

- RanBackhaul $BackhaulDisplayName receive utilization percentage has changed to $BackhaulUtilization, new state is $BackhaulUtilState.
- RanBackhaul $BackhaulDisplayName sent utilization percentage has changed to $BackhaulUtilization, new state is $BackhaulUtilState.

Message Substitution Variables:

Node

Substitution variables for Node related data. This is only valid for real backhaul objects.
Virtual objects will have no associated node data.

BackhaulDisplayName	The name of the backhaul. For a real backhaul this will be of the form 'nodename/backhaulname'. For virtual backhauls there will be no node indicator.
BackhaulUtilState	The current state either Acceptable, Warning or Overloaded.
BackhaulUtilization	The average receive/transmit utilization of link over the last second.

Go Top

SECTION 7.37

Status: SnmpError

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SnmpError	Poll	Alarm	No	Warning	Node $NodeDisplayName has no snmp-able addresses to poll.	SnmpError	IP-RAN
SnmpError	Poll	Alarm	No	Warning	Node $NodeDisplayName is not a supported device or does not have the minimum IOS mib level.	SnmpError	IP-RAN
SnmpError	Poll	Alarm	No	Minor	Node $NodeDisplayName encountered an error during polling: $ErrorString.	SnmpError	IP-RAN
SnmpError	Poll	Alarm	No	Warning	Node $NodeDisplayName has not been configured.	SnmpError	IP-RAN

Description:

The SnmpError status event provides information when MWTM experiences an error during a poll of a Node. The value of SnmpErrorType indicates the type of error. Possible values of SnmpErrorType include:

- NotSnmpable - The Node has no SNMPable interfaces.
- UnsupportedDevice - The Node is not a supported device.
- MibError - An unexpected error occurred.
- NotConfigured - The Node is not configured as an RAN-O device.

Default Message:

- Node $NodeDisplayName has no snmp-able addresses to poll.
- Node $NodeDisplayName is not a supported device or does not have the minimum IOS mib level.
- Node $NodeDisplayName encountered and error during polling: $ErrorString.
- Node $NodeDisplayName has not been configured for a particular MWTM personality.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
SnmpErrorType	Indicates the type of error that occurred.
ErrorString	A detailed error message relative only when ErrorType is MibError.

Operational Information:

- When SnmpErrorType is NotSnmpable check that the Node has not been configured in MWTM to have no SNMPable interfaces. This is most likely a user error.
- When SnmpErrorType is UnsupportedDevice the node is not a supported device or does not have the minimum IOS mib level required by MWTM.
- When SnmpErrorType is MibError an unexpected error has occurred polling a Node. The MessageLog.txt file may have more information related to the error. An ErrorString of 'NoSuchInstance' can occur if MWTM is using a read community string of 'public' for a router but the router has been configured with a non 'public' read community string.
- When SnmpErrorType is NotConfigured the Node is a valid router however it has not been configured for a particular MWTM personality.
- This status could also indicate that device is being accessed via a wrong community string. You can use the MWTM Node SNMP and Credentials Editor to check community strings.

Go Top

SECTION 7.38

Status: PWE3BackhaulStateAdded and PWE3BackhaulStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PWE3BackhaulState	Poll	Alarm	Yes	Normal	PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName added in state Active/ActiveReason.	PWE3BackhaulState	IP-RAN

PWE3BackhaulState	Poll	Alarm	Yes	Normal	PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName changed state from $PWE3BackhaulLastState to Active/ActiveReason.	PWE3BackhaulState	IP-RAN
PWE3BackhaulState	Poll	Alarm	Yes	Warning	PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName added in state Warning/WarningReason.	PWE3BackhaulState	IP-RAN
PWE3BackhaulState	Poll	Alarm	Yes	Informational	PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName added in state $PWE3BackhaulState/$PWE3BackhaulStateReason.	PWE3BackhaulState	IP-RAN
PWE3BackhaulState	Poll	Alarm	Yes	Warning	PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName changed state from $PWE3BackhaulLastState to Warning/WarningReason.	PWE3BackhaulState	IP-RAN
PWE3BackhaulState	Poll	Alarm	Yes	Informational	PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName changed state from $PWE3BackhaulLastState to $PWE3BackhaulState/$PWE3BackhaulStateReason.	PWE3BackhaulState	IP-RAN

Description:

The PWE3BackhaulStateAdded and PWE3BackhaulStateChanged status eventsprovide information when a PWE3Backhaul object is added to the MWTM object model or when MWTM detects that the state of a PWE3Backhaul has changed. The value of PWE3BackhaulState indicates the new state.
Possible values of PWE3BackhaulState include:

- Active - Traffic may flow over this PWE3Backhaul.
- Unknown - The attempt to determine the state of the PWE3Backhaul failed.
- Warning - The PWE3Backhaul is Active however some underlying PWE3VirtualCircuit of this PWE3Backhaul is not fully functional.
- Deleted - The PWE3Backhaul has been deleted from the object database.

Default Message:

- PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName added in state $PWE3BackhaulState/$PWE3BackhaulStateReason.
- PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName changed state from $PWE3BackhaulLastState to $PWE3BackhaulState/$PWE3BackhaulStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.
PWE3BackhaulDisplayName	The name of the PWE3Backhaul.
PWE3BackhaulState	The current state of the PWE3Backhaul.
PWE3BackhaulStateReason	The current state reason of of the PWE3Backhaul.
PWE3BackhaulLastState	The previous state of the PWE3Backhaul.

Operational Information:

See also:

Go Top

SECTION 7.39

Trap: ciscoIpRanBackhaulGsmAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IpRanBackHaulGsmAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is $BackhaulGsmAlarmConnectState, LocalState is $BackhaulGsmAlarmLocalState, Remote State is $BackhaulGsmAlarmRemoteState and RedundancyState is $BackhaulGsmAlarmRedundancyState.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Normal	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Connected, LocalState is Green, Remote State is Green and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Connected, LocalState is Blue, Remote State is Red and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Connected, LocalState is Blue, Remote State is Blue and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN

IpRanBackHaulGsmAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Connected, LocalState is Blue, Remote State is Green and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Connected, LocalState is Green, Remote State is Blue and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Connected, LocalState is Red, Remote State is Red and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Connected, LocalState is Red, Remote State is Blue and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Connected, LocalState is Green, Remote State is Red and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Disconnected, LocalState is Green, Remote State is Green and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Disconnected, LocalState is Green, Remote State is Unavailable and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Disconnected, LocalState is Red, Remote State is Unavailable and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Disconnected, LocalState is Red, Remote State is Red and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is RecConnect, LocalState is Blue, Remote State is Unavailable and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is SendConnect, LocalState is Blue, Remote State is Unavailable and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is SendConnect, LocalState is Green, Remote State is Unavailable and RedundancyState is Active.	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr): ConnectState is ConnectionRejected and Redundancy State is Active	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr): ConnectState is ConnectionAck and Redundancy State is Active	IpRanBackHaulGsmAlarm	IP-RAN
IpRanBackHaulGsmAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr): ConnectState is ConnectedCheck and Redundancy State is Active.	IpRanBackHaulGsmAlarm	IP-RAN

Description:

This trap provide information when the connection state, local alarm state or remote alarm state changes on a gsm interface. Possible values of connection state include:

- connected - The device is monitoring local and remote alarm status.
- disconnected - The system ignores the local alarm status. The local transmitter on the short-haul is disabled. Capability messages are transmitted to the remote describing the provisioning. The system stays disconnected until the remote capabilities are known and the peer state is transitioned to connected.
- sendConnect - One or more attempts have been made to connect to remote peer.
- recConnect - The local-peer has received a connect request from the remote-peer.
- connectedRej - Connection was rejected.
- recConnect - The local-peer has received a connect request from the remote-peer.
- ackConnect - The initial connect request was sent and acknowledged by remote-peer. The local-peer is now waiting for a connect request from the remote-peer.
- connectedCheck - The local-peer has reason to believe its remote-peer has failed. Additonal tests are being processed to verify peer's state.

Possible values of local alarm state and remote alarm state include:

- blue - Indicates a problem at the remote end.
- green - No alarm.
- red - Indicates local interface problem. A-bis: The interface has not received synchronization from the GSM device. Device stops transmitting backhaul samples .
- yellow - The local device signals a receive problem. The remote device stops transmitting backhaul data and indicates a blue alarm.
- unavailable - Indicates the alarms state is not available. This state only applies to remote and occurs when peer connection is inactive.
- txRai - Transmitter is Sending Remote Alarm.

Default Message:

$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is $BackhaulGsmAlarmConnectState, LocalState is $BackhaulGsmAlarmLocalState, Remote State is $BackhaulGsmAlarmRemoteState and RedundancyState is $BackhaulGsmAlarmRedundancyState.

Message Substitution Variables:

CommonNode

Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the MWR router that sent the trap.

BackhaulGsmAlarmConnectState	The current value of the backhaul connection state.
BackhaulGsmAlarmLocalState	The current value of the local alarm state on a gsm interface.
BackhaulGsmAlarmRemoteState	The current value of the remote alarm state on a gsm interface.
BackhaulGsmAlarmRedundancyState	The current value of the redundancy state.
IfAlias	The interface alias.
IfName	The interface name.
IfNumber	The interface number.

Go Top

SECTION 7.40

Trap: ciscoIpRanBackhaulUmtsAlarm

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is $BackhaulUmtsConnectState, Local Receive State is $BackhaulAlarmRxLocalState, Local Transmit State is $BackhaulAlarmTxLocalState, Remote Receive State is $BackhaulAlarmRxRemoteState, Remote Transmit State is $BackhaulAlarmTxRemoteState and RedundancyState is $BackhaulUmtsConnRedundancyState.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Normal	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Open, Local Receive State is Green, Local Transmit State is Green, Remote Receive State is Green, Remote Transmit State is Green and RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Open, Local Receive State is Red, Local Transmit State is Green, Remote Receive State is Green, Remote Transmit State is Green and RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Open, Local Receive State is Red, Local Transmit State is Green, Remote Receive State is Red, Remote Transmit State is Green and RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Open, Local Receive State is Green, Local Transmit State is Green, Remote Receive State is Red, Remote Transmit State is Green and RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Stopped, Local Receive State is Green, Local Transmit State is Green, Remote Receive State is Unavailable, Remote Transmit State is Unavailable and RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Init, RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Starting, RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Closed, RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Stopped, RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Critical	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Closing, RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is Stopping, RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is ConnectSent, Redundancy State is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is AckReceived, RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN
IpRanBackHaulUmtsAlarm	Trap	Event	No	Major	$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is AckSent, Local Receive State is Green, Local Transmit State is Green, Remote Receive State is Unavailable, Remote Transmit State is Unavailable and RedundancyState is Active.	IpRanBackHaulUmtsAlarm	IP-RAN

Description:

This trap provide information when the connection state, local(rx/tx) alarm state or remote(rx/tx) alarm state changes on a gsm interface. Possible values of connection state include:

- init - The connection is starting initilization process.

- starting - The shorthaul interface is administratively active but the backhaul interface is down.
- closed - The backhaul interface is active but shorthaul is administratively closed.
- stopped - Unable to connect to peer in specified time interval. Additional attempts will be tried based on peer request or restart timers.
- closing - Connection ended by administration request.
- stopping - Connection shutdown by peer's Term-Request. Will transition to stopped state.
- connectSent - Connection request sent to peer.
- ackReceived - Connection request sent and acknowledged has been received from peer. Now waiting for peer's connection request.
- ackSent - Connection request received and acknowledged has been sent to peer. Connection request sent and waiting for peer's acknowledgement.
- open - Connection open and available for traffic.

Possible values of local(rx/tx) alarm state and remote(rx/tx) alarm state include:

- blue - Indicates a problem at the remote end.
- green - No alarm.
- red - Indicates local interface problem. A-bis: The interface has not received synchronization from the GSM device. Device stops transmitting backhaul samples .
- yellow - The local device signals a receive problem. The remote device stops transmitting backhaul data and indicates a blue alarm.
- unavailable - Indicates the alarms state is not available. This state only applies to remote and occurs when peer connection is inactive.
- txRai - Transmitter is Sending Remote Alarm.

Default Message:

$NodeDisplayName Interface $IfNumber($IfDescr):ConnectState is $BackhaulUmtsConnectState, Local Receive State is $BackhaulAlarmRxLocalState, Local Transmit State is $BackhaulAlarmTxLocalState, Remote Receive State is $BackhaulAlarmRxRemoteState, Remote Transmit State is $BackhaulAlarmTxRemoteState and RedundancyState is $BackhaulUmtsConnRedundancyState.

Message Substitution Variables:

CommonNode

Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the MWR router that sent the trap.

BackhaulUmtsConnectState	The current value of the backhaul connection state.
BackhaulAlarmRxLocalState	The current value of the local Rx alarm state on a umts interface.
BackhaulAlarmTxLocalState	The current value of the local Tx alarm state on a umts interface.
BackhaulGsmAlarmRxRemoteState	The current value of the remote Rx alarm state on a umts interface.
BackhaulGsmAlarmTxRemoteState	The current value of the remote Tx alarm state on a umts interface.
BackhaulGsmAlarmRedundancyState	The current value of the redundancy state.
IfAlias	The interface alias.
IfName	The interface name.
IfNumber	The interface number.

Go Top

SECTION 7.41

Trap: ospfOriginateLsa

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
OspfOriginateLsa	Trap	Event	No	Informational	$NodeDisplayName -- OSPF LSA originated due to a topology change. Link state DB entry: Area: $ospfLsdbAreaId, Type: $ospfLsdbType, LsId $ospfLsdbLsid, Router Id: $ospfLsdbRouterId	OspfOriginateLsa	IP-RAN

Description:

```
An ospfOriginateLsa trap signifies that a new            LSA has been originated by this router.  This
trap should not be invoked for simple refreshes
of LSAs (which happens every 30 minutes), but
instead will only be invoked when an LSA is
(re)originated due to a topology change.
Additionally, this trap does not include LSAs that
are being flushed because they have reached
MaxAge.
```

Default Message:

$NodeDisplayName - OSPF LSA originated due to a topology change. Link state DB entry: Area: $ospfLsdbAreaId, Type: $ospfLsdbType, LsId $ospfLsdbLsid, Router Id: $ospfLsdbRouterId

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router from which the trap had been sent.
ospfLsdbType	The type of the link state advertisement. Each link state type has a separate advertisement format. Note: External link state advertisements are permitted for backward compatibility, but should be displayed in the ospfAsLsdbTable rather than here. INTEGER is unknown
ospfRouterId	A 32-bit integer uniquely identifying the router in the Autonomous System. By convention, to ensure uniqueness, this should default to the value of one of the router's IP interface addresses. This object is persistent and when written the entity SHOULD save the change to non-volatile storage.
ospfLsdbAreaId	The 32-bit identifier of the area from which the LSA was received.
ospfLsdbLsid	The Link State ID, an LS Type Specific field containing either a Router ID or an IP address; it identifies the piece of the routing domain that is being described by the advertisement.
ospfLsdbRouterId	The 32-bit number that uniquely identifies the originating router in the Autonomous System.

Go Top

SECTION 7.42

Trap: crepLinkStatus

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
REP-IfLinkState	Trap	Event	No	Warning	REP is not operational on the Interface.	REP-IfLinkState	IP-RAN
REP-IfLinkState	Trap	Event	No	Informational	Initial REP link state.	REP-IfLinkState	IP-RAN
REP-IfLinkState	Trap	Event	No	Informational	This is a state in which REP is yet to discover its neighbor.	REP-IfLinkState	IP-RAN
REP-IfLinkState	Trap	Event	No	Informational	REP received messages from the neighbor but the link has not been declared to be twoWay yet.	REP-IfLinkState	IP-RAN
REP-IfLinkState	Trap	Event	No	Informational	REP is in fully operational.	REP-IfLinkState	IP-RAN
REP-IfLinkState	Trap	Event	No	Warning	REP received mismatch port information for the neighbor.	REP-IfLinkState	IP-RAN
REP-IfLinkState	Trap	Event	No	Warning	REP forced transient state before it starts discovering its neighbor.	REP-IfLinkState	IP-RAN
REP-IfLinkState	Trap	Event	No	Critical	REP link state cannot be determined.	REP-IfLinkState	IP-RAN

Description:

```
This notification is sent when a REP interface has entered or        left REP link operational status.  The link is considered
operational when 'crepIfOperStatus' is 'twoWay'.
'crepIfOperStatus' would be 'none' if the
crepInterfaceConfigEntry entry has been removed.
```

Default Message:

crepIfOperStatus :
1. none :
$NodeDisplayName - REP is not operational on the Interface.
2. initDown :
$NodeDisplayName - Initial REP link state.

3. noNeighbor :
$NodeDisplayName - This is a state in which REP is yet to discover its neighbor.
4. oneWay :
$NodeDisplayName - REP received messages from the neighbor but the link has not been declared to be twoWay yet.
5. twoWay :
$NodeDisplayName - REP is in fully operational.
6. flapping :
$NodeDisplayName - REP received mismatch port information for the neighbor.
7. wait :
$NodeDisplayName - REP forced transient state before it starts discovering its neighbor.
8. unknown :
$NodeDisplayName - REP link state cannot be determined.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
crepIfOperStatus	This object indicates the current operational link state of the REP port. If a REP configured interface is down, it will be in 'initDown' state. 'none' - REP is not operational on the interface. This value is used when sending the crepLinkStatus notification when REP configuration is removed from the interface. 'initDown' - initial REP link state. 'noNeighbor' - state in which REP is yet to discover its neighbor. 'oneWay' - the state in which messages have been received from the neighbor but the link has not been declared to be twoWay yet. 'twoWay' - the fully operational state for REP. 'flapping' - the state in which there is a mismatch in the received port information (either local or remote) for the neighbor. 'wait' - the forced transient state before REP starts discovering its neighbor. 'unknown' - the link state cannot be determined. INTEGER is unknown
crepIfSegmentId	This object specifies the segment that the interface is part. This object can be modified when crepIfConfigRowStatus is 'active'. The valid range is from crepMinSegmentId to crepMaxSegmentId.
crepIfIndex	This object identifies the ifIndex-value assigned to the interface.

Go Top

SECTION 7.43

Trap: crepPortRoleChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
REP-VLANPortRoleState	Trap	Event	No	Critical	REP port Link status is in non-operational state, no traffic is forwarded on it.	REP-VLANPortRoleState	IP-RAN
REP-VLANPortRoleState	Trap	Event	No	Informational	REP port link status is alternatePort for forwarding traffic only for a subset of VLANs.	REP-VLANPortRoleState	IP-RAN
REP-VLANPortRoleState	Trap	Event	No	Informational	REP port forwarding traffic for all VLANs.	REP-VLANPortRoleState	IP-RAN

Description:

```
This notification is sent when the role of a Port changes       that are indicated by 'crepIfPortRole'.
```

Default Message:

crepIfPortRole :
1. failedPort :
$NodeDisplayName - REP port link status is in non-operational state, no traffic is forwarded on it.
2. alternatePort :
$NodeDisplayName - REP port link status is alternatePort for forwarding traffic only for a subset of VLANs.
3. openPort :
$NodeDisplayName - REP port forwarding traffic for all VLANs.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
crepIfPortRole	This object indicates the role or state of a REP port depending on its link status and whether it is forwarding or blocking traffic. 'failedPort' - a port with a non-operational link status, such that no traffic is forwarded on it. 'alternatePort' - a port forwarding traffic only for a subset of VLANs, for the purpose of VLAN load balancing. 'openPort' - a port forwarding traffic for all VLANs. INTEGER is unknown
crepIfSegmentId	This object specifies the segment that the interface is part. This object can be modified when crepIfConfigRowStatus is 'active'. The valid range is from crepMinSegmentId to crepMaxSegmentId.
crepIfIndex	This object identifies the ifIndex-value assigned to the interface.

Go Top

SECTION 7.44

Trap: crepPreemptionStatus

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
REP-PreemptionState	Trap	Event	No	Informational	REP primary edge preemption trigger is not executed.	REP-PreemptionState	IP-RAN
REP-PreemptionState	Trap	Event	No	Informational	REP primary edge preemption action for the previous trigger is successful.	REP-PreemptionState	IP-RAN
REP-PreemptionState	Trap	Event	No	Warning	REP primary edge preemption failed due to some problem on the segment.	REP-PreemptionState	IP-RAN
REP-PreemptionState	Trap	Event	No	Informational	REP primary edge preemption trigger is successful and the result is awaited.	REP-PreemptionState	IP-RAN
REP-PreemptionState	Trap	Event	No	Warning	REP primary edge preemption trigger failed, due to invalid port ID.	REP-PreemptionState	IP-RAN

Description:

```
This notification indicates the status of the preemption       triggered on REP primary edge.
```

Default Message:

crepSegmentPreemptStatus :
1. none :
$NodeDisplayName - REP primary edge preemption trigger is not executed.
2. preemptSuccessful :
$NodeDisplayName - REP primary edge preemption action for the previous trigger is successful.
3. preemptFailure :
$NodeDisplayName - REP primary edge preemption failed due to some problem on the segment.

4. preemptTrigger :
$NodeDisplayName - REP primary edge preemption trigger is succesful and the result is awaited.
5. preemptTriggerFailure :
$NodeDisplayName - REP primary edge preemption trigger failed due to invalid port ID.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
crepSegmentPreemptStatus	This object indicates the status of the last preemption trigger. 'none' - preemption trigger is not executed. 'preemptSuccessful' - preemption action for the previous trigger is successful. 'preemptFailure' - preemption trigger was successful. However, preemption failed due to some problem on the segment. 'preemptTrigger' - preemption is triggered successfully and the result is awaited. 'preemptTriggerFailure'- preemption on the segment is not performed as the preemption trigger failed. The failure could be due to invalid port ID or neighbor number specified in 'crepBlockPortNumInfo' or 'crepBlockPortIdInfo' respectively, when the value of 'crepLoadBalanceBlockPortType' is 'offset' or 'portId' respectively. In addition, reason for failure can be that crepLoadBalanceBlockPortType = 'prefFlag' and there is no REP port in the segment configured as preferred port. The value should be 'none' on all agents other than the one serving as the primary edge for the segment. The value will be 'none' on the agent serving as the primary edge for the segment if preemption trigger is not executed yet. If the device is not capable of assessing the final outcome of preemption trigger, then the state should remain in 'preemptTrigger' state. INTEGER is unknown
crepSegmentId	This object identifies the segment identifier.

Go Top

SECTION 7.45

Status: FolderStateAdded and FolderStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FolderState	Poll	Event	No	Normal	Folder $NodeDisplayName/$FolderDisplayName added in state Active/ActiveReason.	FolderState	IP-RAN
FolderState	Poll	Event	No	Warning	Folder $NodeDisplayName/$FolderDisplayName added in state Warning/WarningReason.	FolderState	IP-RAN
FolderState	Poll	Event	No	Warning	Folder $NodeDisplayName/$FolderDisplayName added in state Unknown/UnknownReason.	FolderState	IP-RAN
FolderState	Poll	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName added in state $FolderState/$FolderStateReason.	FolderState	IP-RAN
FolderState	Poll	Event	No	Normal	Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to Active/ActiveReason.	FolderState	IP-RAN
FolderState	Poll	Event	No	Warning	Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to Warning/WarningReason.	FolderState	IP-RAN
FolderState	Poll	Event	No	Warning	Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to Unknown/UnknownReason.	FolderState	IP-RAN
FolderState	Poll	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to $FolderState/$FolderStateReason.	FolderState	IP-RAN

Description:

The FolderStateAdded and FolderStateChanged status events provide information when a Folder object is added to the MWTM object model or when MWTM detects that the state of a Folder has changed. The value of FolderState indicates the new state.
Possible values of FolderState include:

- Active - The Folder is available and is active. This state implies that all the Interfaces in contained in that folder are in the active state.
- Warning - The Folder is Active however some Interfaces belonging to this Folder is not fully functional.
- Unknown - The attempt to determine the state of the Folder failed.

Default Message:

- Folder $NodeDisplayName/$FolderDisplayName added in state $FolderState/$FolderStateReason.
- Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to $FolderState/$FolderStateReason.

Message Substitution Variables:

Nodeof the Folder.

Substitution variables for Node related data.	
FolderState	The current state of the Folder.
FolderStateReason	The current state reason of the Folder.
FolderLastState	The previous state of the Folder.

Operational Information:

- If the current state of the Folder is Active no additional action is necessary.
- If the current state of the Folder is Unknown this is an indicator that one of several events has occurred.
  - An error occurred polling the Node that this Folder belongs to. See the description of the #nodeUnknown Unknown state for a Node for possible causes. for possible causes.
- If the current state of the Folder is Warning this is an indication that one of the objects contained in the folder has a state other than active. You could use the Folder details window to determine the object at error.

Go Top

SECTION 7.46

Status: VirtualBackhaulStateAdded and VirtualBackhaulStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
VirtualBackhaulState	Poll	Event	No	Normal	Virtual Backhaul $VirtualBackhaulDisplayName added in state Active/ActiveReason.	VirtualBackhaulState	IP-RAN
VirtualBackhaulState	Poll	Event	No	Warning	Virtual Backhaul $VirtualBackhaulDisplayName added in state Warning/WarningReason.	VirtualBackhaulState	IP-RAN
VirtualBackhaulState	Poll	Event	No	Warning	Virtual Backhaul $VirtualBackhaulDisplayName added in state Unknown/UnknownReason.	VirtualBackhaulState	IP-RAN
VirtualBackhaulState	Poll	Event	No	Informational	Virtual Backhaul $VirtualBackhaulDisplayName added in state $VirtualBackhaulState/$VirtualBackhaulStateReason.	VirtualBackhaulState	IP-RAN
VirtualBackhaulState	Poll	Event	No	Normal	Virtual Backhaul $VirtualBackhaulDisplayName changed state from $VirtualBackhaulLastState to Active/ActiveReason.	VirtualBackhaulState	IP-RAN
VirtualBackhaulState	Poll	Event	No	Warning	Virtual Backhaul $VirtualBackhaulDisplayName changed state from $VirtualBackhaulLastState to Warning/WarningReason.	VirtualBackhaulState	IP-RAN
VirtualBackhaulState	Poll	Event	No	Warning	Virtual Backhaul $VirtualBackhaulDisplayName changed state from $VirtualBackhaulLastState to Unknown/UnknownReason.	VirtualBackhaulState	IP-RAN
VirtualBackhaulState	Poll	Event	No	Informational	Virtual Backhaul $VirtualBackhaulDisplayName changed state from $VirtualBackhaulLastState to $VirtualBackhaulState/$VirtualBackhaulStateReason.	VirtualBackhaulState	IP-RAN

Description:

The VirtualBackhaulStateAdded andVirtualBackhaulStateChanged status events provide information when a Virtual Backhaul object is added to the MWTM object model or when MWTM detects that the state of a Virtual Backhaul has changed. The value of VirtualbackhaulState indicates the

new state. Possible values of VirtualbackhaulState include:

- Active - Traffic may flow over this Virtual Backhaul.
- Unknown - The attempt to determine the state of the Virtual Backhaul failed.
- Warning - The Virtual Backhaul is Active however some underlying RanBackhaul ofthis Virtual Backhaul is not fully functional.
- Deleted - The Virtual Backhaul has been deleted from the MWTM object database.

Default Message:

- Virtual Backhaul $VirtualBackhaulDisplayName added in state $VirtualBackhaulState/$VirtualBackhaulStateReason.
- Virtual Backhaul $VirtualBackhaulDisplayName changed state from $VirtualBackhaulLastState to $VirtualBackhaulState/$VirtualBackhaulStateReason.

Message Substitution Variables:

Virtual Backhaulof the Virtual Backhaul.

Substitution variables for Virtual Backhaul related data.	
VirtualBackhaulState	The current state of the Virtual Backhaul.
VirtualBackhaulStateReason	The current state reason of the Virtual Backhaul.
VirtualBackhaulLastState	The previous state of the Virtual Backhaul.

Operational Information:

- If the current state of the Virtual Backhaul is Active no additional action is necessary.
- If the current state of the Virtual Backhaul is Unknown this is an indicator that one of several events has occurred.
  - An error occurred determining the state of the Virtual Backhaul.
- If the current state of the Virtual Backhaul is Warning this is an indication that one of the Virtual Backhaul's components has a state other than active. You should use the Virtual Backhaul details window to determine the probable causes.
- When the current state of the Virtual Backhaul is Deleted a MWTM user has manually deleted the Virtual Backhaul.

See also:

- Troubleshooting techniques

Go Top

SECTION 7.47

Status: TrapOutOfSequence

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
TrapOutOfSequence	Poll	Event	No	Minor	$NodeDisplayName ($NodeClliCode) - Trap $SequenceNumber received out of sequence. Last trap received was $LastSequenceNumber.	TrapOutOfSequence	IP-RAN

Description:

The TrapOutOfSequence status event provides information when MWTM determines that a trap generated by a router has not reached MWTM. If successive traps received by MWTM for the same router do not contain successive sequence numbers then this event is generated.

Default Message:

- $NodeDisplayName ($NodeClliCode) - Trap $SequenceNumber received out of sequence. Last trap received was $LastSequenceNumber.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
SequenceNumber	The sequence number of the current trap received by MWTM.
LastSequenceNumber	The sequence of the previous trap received by MWTM.

Operational Information:

- The reception of this event could mean that you have networks problems that are preventing the traps from reaching MWTM. SNMP traps use the UDP protocol and as such can be dropped by the network for various reasons.

Go Top

SECTION 7.48

Status: TL1Error

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
TL1Error	Poll	Event	No	Major	$NodeDisplayName --TL1 Access Error: $TL1ErrorMessage.	TL1Error	IP-RAN

Description:

The TL1Error status event provides information when MWTMexperiences an error during a poll of a Node that requires TL1 access.

Default Message:

- $NodeDisplayName --TL1 Access Error: $TL1ErrorMessage.

Message Substitution Variables:

Node	Substitution variables for Node related data.
TL1ErrorMessage	Describes the type of error that occurred.

Go Top

SECTION 7.49

UserAction: CardIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CardIgnoredSet	User Action	Event	No	Informational	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName ignore flag is set to $IgnoredFlag by $User.	CardIgnoredSet	IP-RAN

Description:

The CardIgnoredSet UserAction event provides information when a Card's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the Card in the aggregation algorithm in determining the state of a Node. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The Card is to be excluded from state aggregation.
- False - The Card is to be included in state aggregation.

Default Message:

Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

CardDisplayName	The name of the Card.
CardSlotNumber	The slot number of the Card.
CardState	The current state of the Card.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

The setting of the ignore flag to True can lead to confusing aggregated Node states. To find the Cards which are currently ignored select the Card folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 7.50

User Action : FolderIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FolderIgnoredSet	User Action	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName ignore flag is set to $IgnoredFlag by $User.	FolderIgnoredSet	IP-RAN

Go Top

SECTION 7.51

UserAction: RanBackhaulIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RanBackhaulIgnoredSet	User Action	Event	No	Informational	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName ignore flag is set to $IgnoredFlag by $User.	RanBackhaulIgnoredSet	IP-RAN

Description:

The RanBackhaulIgnoredSet UserAction event provides information when a RanBackhaul's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the RanBackhaul in the aggregation algorithm in determining the state of a Node. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The RanBackhaul is to be excluded from state aggregation.
- False - The RanBackhaul is to be included in state aggregation.

Default Message:

RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
RanBackhaulDisplayName	The name of the RanBackhaul.
RanBackhaulState	The current state of the RanBackhaul.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated Node states. To find the RanBackhauls which are currently ignored select the RanBackhaul folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 7.52

UserAction: VirtualBackhaulIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
VirtualBackhaulIgnoredSet	User Action	Event	No	Informational	Virtual Backhaul $VirtualBackhaulDisplayName ignore flag is set to $IgnoredFlag by $User.	VirtualBackhaulIgnoredSet	IP-RAN

Description:

The VirtualBackhaulIgnoredSet UserAction event provides information when a Virtual Backhaul's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the Virtual Backhaul in the aggregation algorithm. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The Virtual Backhaul is to be excluded from state aggregation.
- False - The Virtual Backhaul is to be included in state aggregation.

Default Message:

Virtual Backhaul $VirtualBackhaulDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Virtual Backhaul	
Substitution variables for Virtual Backhaul related data.	
VirtualBackhaulState	The current state of the Virtual Backhaul.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the Virtual Backhauls which are currently ignored select the Virtual Backhaul folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 7.53

User Action : CardUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CardUserDataUpdated	User Action	Event	No	Informational	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName edited by user $User.	CardUserDataUpdated	IP-RAN

Go Top

SECTION 7.54

User Action : FolderUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FolderUserDataUpdated	User Action	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName edited by user $User.	FolderUserDataUpdated	IP-RAN

Go Top

SECTION 7.55

UserAction: RanBackhaulUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RanBackhaulUserDataUpdated	User Action	Event	No	Informational	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName edited by user $User.	RanBackhaulUserDataUpdated	IP-RAN

Description:

The RanBackhaulUserDataUpdated UserAction event provides information when a RanBackhaul object's user data has been updated by a MWTM user.

Default Message:

RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName edited by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.

RanBackhaulDisplayName	The name of the RanBackhaul.
User	The user who requested the RanBackhaul's data be updated.

Operational Information:

The fields that can be updated for a RanBackhaul include:

- The RanBackhaul's notes data used for communicating installation dependent information about a RanBackhaul.
- The AcceptableThreshold, WarningThreshold, OverloadedThreshold, and UserBandwidth fields.

Go Top

SECTION 7.56

UserAction: VirtualBackhaulUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
VirtualBackhaulUserDataUpdated	User Action	Event	No	Informational	Virtual Backhaul $VirtualBackhaulDisplayName edited by user $User.	VirtualBackhaulUserDataUpdated	IP-RAN

Description:

The VirtualBackhaulUserDataUpdated UserAction event provides information when a Virtual Backhaul object's user data has been updated by an MWTM user.

Default Message:

Virtual Backhaul $VirtualBackhaulDisplayName edited by user $User.

Message Substitution Variables:

Virtual Backhaul

Substitution variables for Virtual Backhaul related data.

User	The user who requested the Virtual Backhaul's data be updated.

Operational Information:

The fields that can be updated for a Virtual Backhaul include:

- The Virtual Backhaul's notes data used for communicating installationdependent information about a VirtualBackhaul.
- The AcceptableThreshold,WarningThreshold, OverloadedThreshold, and UserBandwidth values for a Virtual Backhaul.

Go Top

SECTION 7.57

UserAction: CardDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CardDeleted	User Action	Event	No	Informational	Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName deleted by user $User.	CardDeleted	IP-RAN

Description:

The CardDeleted UserAction event provides information when an Card object's deletion from the SGM object model database is requested.

Default Message:

Card $NodeDisplayName/$CardSlotNumber - $CardDisplayName deleted by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

CardDisplayName	The name of the Card.
CardSlotNumber	The slot number of the Card.
User	The user who requested the Card's data be deleted.

Operational Information:

- The indicated User can be the user id associated with the server processes. As a part of normal server discovery operations Card objects can be deleted on behalf of the server.

Go Top

SECTION 7.58

User Action : FolderDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FolderDeleted	User Action	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName deleted by user $User.	FolderDeleted	IP-RAN

Go Top

SECTION 7.59

UserAction: RanBackhaulDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RanBackhaulDeleted	User Action	Event	No	Informational	RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName deleted by user $User.	RanBackhaulDeleted	IP-RAN

Description:

The RanBackhaulDeleted UserAction event provides information when a RanBackhaul object's deletion from the MWTM object model database is requested.

Default Message:

RanBackhaul $NodeDisplayName/$RanBackhaulDisplayName deleted by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

RanBackhaulDisplayName	The display name of the RanBackhaul from the MWTM object database.
User	The user who requested the RanBackhaul's data be deleted.

Operational Information:

- The deletion of a RanBackhaul can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 7.60

UserAction: VirtualBackhaulCreated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
VirtualBackhaulCreated	User Action	Event	No	Informational	Virtual Backhaul $VirtualBackhaulDisplayName created by user $User.	VirtualBackhaulCreated	IP-RAN

Description:

The VirtualBackhaulCreated UserAction event provides information when a Virtual Backhaul object's creation in the SGM object model database is requested.

Default Message:

Virtual Backhaul $VirtualBackhaulDisplayName created by user $User.

Message Substitution Variables:

Virtual Backhaul
Substitution variables for Virtual Backhaul related data.

User	The user who requested the Virtual Backhaul's data be created.

Operational Information:

None.
Go Top

SECTION 7.61

UserAction: VirtualBackhaulDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
VirtualBackhaulDeleted	User Action	Event	No	Informational	Virtual Backhaul $VirtualBackhaulDisplayName deleted by user $User.	VirtualBackhaulDeleted	IP-RAN

Description:

The VirtualBackhaulDeleted UserAction event provides information when a Virtual Backhaul object's deletion from the SGM object model database is requested.

Default Message:

Virtual Backhaul $VirtualBackhaulDisplayName deleted by user $User.

Message Substitution Variables:

Virtual Backhaul
Substitution variables for Virtual Backhaul related data.

User	The user who requested the Virtual Backhaul's data be deleted.

Operational Information:

None.
Go Top

SECTION 7.62

UserAction: PWE3BackhaulIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PWE3BackhaulIgnoredSet	User Action	Event	No	Informational	PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName ignore flag is set to $IgnoredFlag by $User.	PWE3BackhaulIgnoredSet	IP-RAN

Description:

The PWE3BackhaulIgnoredSet UserAction event provides information when a PWE3Backhaul's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the PWE3Backhaul in the aggregation algorithm in determining the state of a View. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The PWE3Backhaul is to be excluded from state aggregation.
- False - The PWE3Backhaul is to be included in state aggregation.

Default Message:

PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
PWE3BackhaulDisplayName	The display name of the PWE3Backhaul from the MWTM object database.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Go Top

SECTION 7.63

UserAction: PWE3BackhaulUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PWE3BackhaulUserDataUpdated	User Action	Event	No	Informational	PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName edited by user $User.	PWE3BackhaulUserDataUpdated	IP-RAN

Description:

The PWE3BackhaulUserDataUpdated UserAction event provides information when a PWE3Backhaul object's user data has been updated by a MWTM user.

Default Message:

PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName edited by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
PWE3BackhaulDisplayName	The display name of the PWE3Backhaul from the MWTM object database.
User	The user who requested the PWE3Backhaul's data be updated.

Operational Information:

The fields that can be updated for a PWE3Backhaul include:

- The PWE3Backhaul's notes data used for communicating installation dependent information about a PWE3Backhaul.

Go Top

SECTION 7.64

UserAction: PWE3BackhaulDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PWE3BackhaulDeleted	User Action	Event	No	Informational	PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName deleted by user $User.	PWE3BackhaulDeleted	IP-RAN

Description:

The PWE3BackhaulDeleted UserAction event provides information when a PWE3Backhaul object's deletion from the MWTM object model database is requested.

Default Message:

PWE3Backhaul $NodeDisplayName/$PWE3BackhaulDisplayName deleted by user $User.

Message Substitution Variables:

Node	
Substitution variables for Node related data.	
PWE3BackhaulDisplayName	The display name of the PWE3Backhaul from the MWTM object database.
User	The user who requested the PWE3Backhaul's data be deleted.

Operational Information:

- The deletion of a PWE3Backhaul can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 7.65

UserAction: PWE3VCIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PWE3VCIgnoredSet	User Action	Event	No	Informational	PWE3VC $NodeDisplayName/$PWE3VCDisplayName ignore flag is set to $IgnoredFlag by $User.	PWE3VCIgnoredSet	IP-RAN

Description:

The PWE3VCIgnoredSet UserAction event provides information when a PWE3VirtualCircuit's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the PWE3VirtualCircuit in the aggregation algorithm in determining the state of a View. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The PWE3VirtualCircuit is to be excluded from state aggregation.
- False - The PWE3VirtualCircuit is to be included in state aggregation.

Default Message:

PWE3VC $NodeDisplayName/$PWE3VCDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node	
Substitution variables for Node related data.	
PWE3VCDisplayName	The display name of the PWE3VirtualCircuit from the MWTM object database.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Go Top

SECTION 7.66

UserAction: PWE3VCUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PWE3VCUserDataUpdated	User Action	Event	No	Informational	PWE3VC $NodeDisplayName/$PWE3VCDisplayName edited by user $User.	PWE3VCUserDataUpdated	IP-RAN

Description:

The PWE3VCUserDataUpdated UserAction event provides information when a PWE3VirtualCircuit object's user data has been updated by a MWTM user.

Default Message:

PWE3VC $NodeDisplayName/$PWE3VCDisplayName edited by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

PWE3VCDisplayName	The display name of the PWE3VirtualCircuit from the MWTM object database.
User	The user who requested the PWE3VirtualCircuit's data be updated.

Operational Information:

The fields that can be updated for a PWE3VirtualCircuit include:

- The PWE3VirtualCircuit's notes data used for communicating installation dependent information about a PWE3VirtualCircuit.

Go Top

SECTION 7.67

UserAction: PWE3VCDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PWE3VCDeleted	User Action	Event	No	Informational	PWE3VC $NodeDisplayName/$PWE3VCDisplayName deleted by user $User.	PWE3VCDeleted	IP-RAN

Description:

The PWE3VCDeleted UserAction event provides information when a PWE3VirtualCircuit object's deletion from the MWTM object model database is requested.

Default Message:

PWE3VC $NodeDisplayName/$PWE3VCDisplayName deleted by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

PWE3VCDisplayName	The display name of the PWE3VirtualCircuit from the MWTM object database.
User	The user who requested the PWE3VirtualCircuit's data be deleted.

Operational Information:

- The deletion of a PWE3VirtualCircuit can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 8.1

Trap: titanAlarmStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CDTAlarm	Trap	Alarm	Yes	Normal	$NodeDisplayName -- Subsystem type: $titanAlarmSubsystemType. Subsystem name: $titanAlarmSubsystemName. Alarm type: $titanAlarmAlarmType. Probable cause: $titanAlarmProbableCause. Specific cause: $titanAlarmSpecificCause. Repair action: $titanAlarmRepairAction.	CDTAlarm	ITP
CDTAlarm	Trap	Alarm	Yes	Warning	$NodeDisplayName -- Subsystem type: $titanAlarmSubsystemType. Subsystem name: $titanAlarmSubsystemName. Alarm type: $titanAlarmAlarmType. Probable cause: $titanAlarmProbableCause. Specific cause: $titanAlarmSpecificCause. Repair action: $titanAlarmRepairAction.	CDTAlarm	ITP
					$NodeDisplayName -- Subsystem type: $titanAlarmSubsystemType. Subsystem name: $titanAlarmSubsystemName.		

CDTAlarm	Trap	Alarm	Yes	Minor	Alarm type: $titanAlarmAlarmType. Probable cause: $titanAlarmProbableCause. Specific cause: $titanAlarmSpecificCause. Repair action: $titanAlarmRepairAction.	CDTAlarm	ITP
CDTAlarm	Trap	Alarm	Yes	Major	$NodeDisplayName -- Subsystem type: $titanAlarmSubsystemType. Subsystem name: $titanAlarmSubsystemName. Alarm type: $titanAlarmAlarmType. Probable cause: $titanAlarmProbableCause. Specific cause: $titanAlarmSpecificCause. Repair action: $titanAlarmRepairAction.	CDTAlarm	ITP
CDTAlarm	Trap	Alarm	Yes	Critical	$NodeDisplayName -- Subsystem type: $titanAlarmSubsystemType. Subsystem name: $titanAlarmSubsystemName. Alarm type: $titanAlarmAlarmType. Probable cause: $titanAlarmProbableCause. Specific cause: $titanAlarmSpecificCause. Repair action: $titanAlarmRepairAction.	CDTAlarm	ITP
CDTAlarm	Trap	Alarm	Yes	Indeterminate	$NodeDisplayName -- Subsystem type: $titanAlarmSubsystemType. Subsystem name: $titanAlarmSubsystemName. Alarm type: $titanAlarmAlarmType. Probable cause: $titanAlarmProbableCause. Specific cause: $titanAlarmSpecificCause. Repair action: $titanAlarmRepairAction.	CDTAlarm	ITP

Description:

A titanAlarmStatusChange trap signifies that an errorcondition has occurred or cleared causing a change of status in a TITAN resource. The severity of the alarm is given in titanAlarmSeverity; the alarm identifier, titanAlarmId, is the specific ID of the alarm; the affected subsystem and subsystem type are given in titanAlarmSubsystemName and titanAlarmSubsystemType; the details are given in titanAlarmProbableCause and titanAlarmSpecificCause. The time the alarm occurred, titanAlarmTimestamp, is in UTC Time.

Default Message:

Add default message here.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
titanAlarmSeverity	The severity of the alarm. The perceived severity of an alarm.
titanAlarmAlarmType	The type of the alarm condition. The type of an alarm.
titanAlarmSubsystemType	The type of subsystem that is experiencing the alarm condition. The subsystem associated with the alarm.
titanAlarmId	An integer identifying the alarm. It will not be a zero or negative value. The titanAlarmId is an index into the AlarmTable.
titanAlarmSubsystemName	The name of the subsystem that is experiencing the alarm condition.
titanAlarmProbableCause	The probably cause of the alarm condition.
titanAlarmSpecificCause	A text string containing the details of an alarm condition.
titanAlarmRepairAction	A suggested repair action.
titanAlarmTimestamp	The time, in Universal Time, or UTC, that the alarm occurred. Format is YYYY:MM:DD:HH:mm:ss:Z
titanAlarmSubsystemName	The name of the subsystem that is experiencing the alarm condition.
titanAlarmId	An integer identifying the alarm. It will not be a zero or negative value. The titanAlarmId is an index into the AlarmTable.

Go Top

SECTION 8.2

Trap: cItpSpLinksetStateChange and ciscoGspLinksetStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinksetState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Linkset $LinksetName : linkset is $LinksetState.	LinksetState	ITP
LinksetState	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Linkset $LinksetName : linkset is $LinksetState.	LinksetState	ITP
LinksetState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Linkset $LinksetName : linkset is $LinksetState.	LinksetState	ITP
LinksetState	Poll	Alarm	Yes	Normal	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName added in state Active/ActiveReason.	LinksetState	ITP
LinksetState	Poll	Event	Yes	Warning	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName added in state Warning/WarningReason.	LinksetState	ITP
LinksetState	Poll	Alarm	Yes	Warning	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName added in state Shutdown/ShutdownReason.	LinksetState	ITP
LinksetState	Poll	Alarm	Yes	Major	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName added in state Unavailable/UnavailableReason.	LinksetState	ITP
LinksetState	Poll	Event	Yes	Informational	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName added in state $LinksetState/$LinksetStateReason.	LinksetState	ITP
LinksetState	Poll	Alarm	Yes	Normal	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName changed state from $LinksetLastState to Available/AvailableReason.	LinksetState	ITP
LinksetState	Poll	Alarm	Yes	Normal	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName changed state from $LinksetLastState to Active/ActiveReason.	LinksetState	ITP
LinksetState	Poll	Event	Yes	Warning	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName changed state from $LinksetLastState to Warning/WarningReason.	LinksetState	ITP
LinksetState	Poll	Alarm	Yes	Warning	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName changed state from $LinksetLastState to Shutdown/ShutdownReason.	LinksetState	ITP
LinksetState	Poll	Alarm	Yes	Major	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName changed state from $LinksetLastState to Unavailable/UnavailableReason.	LinksetState	ITP
LinksetState	Poll	Event	Yes	Warning	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName changed state from $LinksetLastState to Unknown/UnknownReason.	LinksetState	ITP
LinksetState	Poll	Event	Yes	Informational	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName changed state from $LinksetLastState to $LinksetState/$LinksetStateReason.	LinksetState	ITP

Description:

These traps provide information when a linkset changes to a new state. The value of LinksetState indicates the new state. Possible values of LinksetState include:

- Available - Traffic may flow over this linkset.
- Shutdown - This linkset has been forced to an unavailable state by an administrative action.
- Unavailable - The linkset is currently unable to support traffic. Activation of this linkset will occur as required by protocol.

Default Message:

$NodeDisplayName ($NodeClliCode) $SpDisplayName - Linkset $LinksetName : linkset is $LinksetState.

Message Substitution Variables:

CommonNodeSignalingPointLinksetLink

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
Substitution variables for Link related data.	
LinksetName	The name of the Linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetLocalPointCode	The local point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetAdjacentPointCode	The adjacent point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetState	The state change value of the linkset extracted from the trap PDU.
SequenceNumber	For the cItpSpLinksetStateChange trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the state of the linkset is 'Available' then no action is necessary.
- If the state of the linkset is 'Shutdown' this is an indication that an operator issued a 'shut' command on the ITP router to shutdown this linkset.
- If the state of the linkset is 'Unavailable' then either the underlying links are unavailable on this ITP router or the linkset on the adjacent node has been shutdown or become unavailable because it's underlying links are unavailable.
- If the state of linkset is 'Unavailable' it could also indicate physical connectivity problems. Communication to ITP could be out-of-service or is congested.

Diagnostic Commands:

To display information about the current state of the links in the linkset use command:

show cs7 [instance-number] linkset [*ls-name* statistics | state | utilization]

ls-name	(Optional) Linkset name. Displays information for this particular linkset.
statistics	(Optional) Displays link usage statistics.
state	(Optional) Displays MTP3 states for link.
utilization	(Optional) Displays link utilization statistics.

See also:

- Troubleshooting techniques

Go Top

SECTION 8.3

Trap: ciscoGspLinkStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCllliCode) $SpDisplayName - Link $LinksetName/$SLC: link is Available.	LinkState	ITP
LinkState	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCllliCode) $SpDisplayName - Link $LinksetName/$SLC: link has Shutdown.	LinkState	ITP
LinkState	Trap	Alarm	Yes	Critical	$NodeDisplayName ($NodeCllliCode) $SpDisplayName - Link $LinksetName/$SLC: link has Failed / $LinkStateReason / $LinkTestResult.	LinkState	ITP
LinkState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCllliCode) $SpDisplayName - Link $LinksetName/$SLC: link is Unavailable / $LinkStateReason / $LinkTestResult.	LinkState	ITP
LinkState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCllliCode) $SpDisplayName - Link $LinksetName/$SLC: link state is Unknown / $LinkStateReason / $LinkTestResult.	LinkState	ITP
LinkState	Poll	Event	Yes	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state $LinkState/$LinkStateReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Normal	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state Active/ActiveReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Major	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state Blocked/BlockedReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Critical	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state Failed/FailedReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Major	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state Unavailable/UnavailableReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state InhibitLoc/InhibitLocReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state InhibitRem/InhibitRemReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Warning	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state Shutdown/ShutdownReason.	LinkState	ITP
LinkState	Poll	Event	Yes	Warning	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state Warning/WarningReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC added in state InhibitLocRem/InhibitLocRemReason.	LinkState	ITP
LinkState	Poll	Event	Yes	Normal	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to Active/ActiveReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Normal	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to Available/AvailableReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Major	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to Blocked/BlockedReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Critical	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to Failed/FailedReason.	LinkState	ITP

LinkState	Poll	Alarm	Yes	Major	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to Unavailable/UnavailableReason.	LinkState	ITP
LinkState	Poll	Event	Yes	Major	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to Unknown/UnknownReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to InhibitLoc/InhibitLocReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to InhibitRem/InhibitRemReason.	LinkState	ITP
LinkState	Poll	Event	Yes	Warning	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to Warning/WarningReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to InhibitLocRem/InhibitLocRemReason.	LinkState	ITP
LinkState	Poll	Event	Yes	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to $LinkState/$LinkStateReason.	LinkState	ITP
LinkState	Poll	Alarm	Yes	Warning	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC changed state from $LinkLastState to Shutdown/ShutdownReason.	LinkState	ITP

Description:

The ciscoGspLinkStateChange trap provides information when a link changes to a new state. The value of LinkState indicates the new state. Possible values of LinkState include:

- Available - Traffic may flow over this link.
- Failed - Traffic management has detected a failure that prevents activating this link.
- Shutdown - This link has been forced to an unavailable state by an administrative action.
- Unavailable - The link is currently unable to support traffic. Activation of this linkset will occur as required by protocol.

For LinkState values of Failed and Unavailable there are 2 state modifiers:

- LinkStateReason - This object provides additional - This object provides additional information on the source of a link failure and will contain the last reason that caused the link to fail.
- LinkTestResult - This object provides information on - This object provides information on result from signaling link test procedures.

This trap conforms to Q.752 T5E1 and T5E3 notifications.

Default Messages:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: link is Available.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: link has Shutdown.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: link has Failed / $LinkStateReason / $LinkTestResult.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: link is Unavailable / $LinkStateReason / $LinkTestResult.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: link state is Unknown.

Message Substitution Variables:

CommonNodeSignalingPointLinksetLink

Substitution variables common to all traps.

Substitution variables for Node related data. The Node is obtained from the MWTM database
based on the IP address of the ITP router that sent the trap.

Substitution variables for SignalingPoint related data.

Substitution variables for Linkset related data.

Substitution variables for Link related data.

LinksetName	The name of the Linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetLocalPointCode	The local point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetAdjacentPointCode	The adjacent point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinkState	The state change value of the link extracted from the trap PDU.
LinkStateReason	The state change reason value of the link extracted from the trap PDU.
LinkTestResult	The result of a signaling link test extracted from the trap PDU.
SLC	The SLC id value of the link extracted from the trap PDU.
SequenceNumber	SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the state of the link is 'Available' then no action is necessary.
- If the state of the link is 'Failed' this is an indication that the underlying interfaces are unavailable on this ITP router or the link on the adjacent node has been shutdown or become unavailable because it's underlying interfaces are unavailable.
- If the state of the link is 'Shutdown' this is an indication that an operator issued a 'shut' command on the ITP router to shutdown this link.

Diagnostic Commands:

To display information about the current state of the links in the linkset use command:

show cs7 [instance-number] linkset [*ls-name* statistics | state | utilization]

ls-name	(Optional) Linkset name. Displays information for this particular linkset.
statistics	(Optional) Displays link usage statistics.
state	(Optional) Displays MTP3 states for link.
utilization	(Optional) Displays link utilization statistics.

See also:

- Additional Troubleshooting Techniques

Go Top

SECTION 8.4

Trap: cItpSpCongestionChange and ciscoGspCongestionChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkCongestionChange	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is None.	LinkCongestionChange	ITP
LinkCongestionChange	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is Low.	LinkCongestionChange	ITP
LinkCongestionChange	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is High.	LinkCongestionChange	ITP
LinkCongestionChange	Trap	Alarm	Yes	Critical	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is Very High.	LinkCongestionChange	ITP
LinkCongestionChange	Trap	Alarm	Yes	Critical	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is $CongestionState ($Varbind1).	LinkCongestionChange	ITP
LinkCongestionChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is None.	LinkCongestionChange	ITP
LinkCongestionChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is Low.	LinkCongestionChange	ITP
LinkCongestionChange	Poll	Alarm	Yes	Major	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is High.	LinkCongestionChange	ITP
LinkCongestionChange	Poll	Alarm	Yes	Critical	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is Very High.	LinkCongestionChange	ITP
LinkCongestionChange	Poll	Alarm	Yes	Critical	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is $CongestionState.	LinkCongestionChange	ITP

Description:

These traps provide information when a link changes to a new congestion state based on the number of MSU's waiting to be sent. The value of CongestionState indicates the new state. Possible values of CongestionState include:

- none - no congestion.
- low - congestion level 1 as defined via mtp3 tuning parameters on the ITP router.
- high - congestion level 2 as defined via mtp3 tuning parameters on the ITP router.
- very_high - congestion level 3 as defined via mtp3 tuning parameters on the ITP router.

Default Message:

$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: link congestion level is $CongestionState.

Message Substitution Variables:

CommonNodeSignalingPointLinksetLink

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
Substitution variables for Link related data.	
LinksetName	The name of the Linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetLocalPointCode	The local point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetAdjacentPointCode	The adjacent point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
SLC	The SLC id value of the link extracted from the trap PDU.
CongestionState	The current level of congestion of the link extracted from the trap PDU.
SequenceNumber	For the ciscoGspCongestionChange trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the congestion level of the link is 'none' then no action is necessary.
- If the congestion level of the link is 'low', 'high', or 'very_high' then you may want to add few links or look at rerouting some traffic across other links.

Diagnostic Commands:

To display information about the current state of the links in the linkset use command:

show cs7 [instance-number] linkset [*ls-name* statistics | state | utilization]

ls-name	(Optional) Linkset name. Displays information for this particular linkset.
statistics	(Optional) Displays link usage statistics.
state	(Optional) Displays MTP3 states for link.
utilization	(Optional) Displays link utilization statistics.

Go Top

SECTION 8.5

Trap: cItpSpLinkRcvdUtilChange and cItpSpLinkSentUtilChange ciscoGspLinkRcvdUtilChange and ciscoGspLinkSentUtilChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkReceivedUtilChange	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Receive utilization is overThreshold at $UtilizationPercent% .	LinkReceivedUtilChange	ITP
LinkReceivedUtilChange	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Receive utilization is underThreshold at $UtilizationPercent% .	LinkReceivedUtilChange	ITP
LinkReceivedUtilChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Receive utilization is OverThreshold.	LinkReceivedUtilChange	ITP
LinkReceivedUtilChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Receive utilization is Unmonitored.	LinkReceivedUtilChange	ITP
					$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Receive		

LinkReceivedUtilChange	Poll	Alarm	Yes	Normal	utilization is UnderThreshold.	LinkReceivedUtilChange	ITP

Description:

These traps notify network management applications of changes in link utilization. The Utilization state indicates either under or over defined thresholds as follows:

- overThreshold - utilization has exceeded the configured threshold level.
- underThreshold - utilization has returned to below the configured threshold abatement level.

Default Message:

- $NodeDisplayName ($NodeCliliCode) $SpDisplayName - Link $LinksetName/$SLC: Receive utilization is $UtilizationState at $UtilizationPercent% .
- $NodeDisplayName ($NodeCliliCode) $SpDisplayName - Link $LinksetName/$SLC: Send utilization is $UtilizationState at $UtilizationPercent% .

Message Substitution Variables:

CommonNodeSignalingPointLinksetLink

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
Substitution variables for Link related data.	
LinksetName	The name of the Linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetLocalPointCode	The local point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetAdjacentPointCode	The adjacent point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
SLC	The SLC id value of the link extracted from the trap PDU.
UtilizationState	The current threshold position either overThreshold or underThreshold.
UtilizationPercent	The current percentage of utilization for the link based on the capacity and bytes sent or received.
SequenceNumber	For the ciscoGspLinkRcvdUtilChange and ciscoGspLinkSentUtilChange traps only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the utilization state is 'underThreshold' then no action is necessary.
- If the utilization state is 'overThreshold' then you may want to add few links or look at rerouting some traffic across other links. At certain points in time the UtilizationPercent may exceed 100% due to timing considerations during utilization calculation. UtilizationPercent's of 999% can most often be ignored unless it occurs excessively. UtilizationPercent can also exceed 100% when the planned capacity specified on the ITP router for a link is specified as less than the actual capacity of the link.
- If the traffic in the links exceeds specified values, it can indicate that ITP may not be able to handle traffic if mate fails.

Diagnostic Commands:

To display information about the current state of the links in the linkset use command:

show cs7 [instance-number] linkset [*ls-name* statistics | state | utilization]

ls-name	(Optional) Linkset name. Displays information for this particular linkset.
statistics	(Optional) Displays link usage statistics.
state	(Optional) Displays MTP3 states for link.
utilization	(Optional) Displays link utilization statistics.

Go Top

Trap: cItpSpLinkRcvdUtilChange and cItpSpLinkSentUtilChange ciscoGspLinkRcvdUtilChange and ciscoGspLinkSentUtilChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkSentUtilChange	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Send utilization is overThreshold at $UtilizationPercent% .	LinkSentUtilChange	ITP
LinkSentUtilChange	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Send utilization is underThreshold at $UtilizationPercent% .	LinkSentUtilChange	ITP
LinkSentUtilChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Send utilization is OverThreshold.	LinkSentUtilChange	ITP
LinkSentUtilChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Send utilization is Unmonitored.	LinkSentUtilChange	ITP
LinkSentUtilChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Send utilization is UnderThreshold.	LinkSentUtilChange	ITP

Description:

These traps notify network management applications of changes in link utilization. The Utilization state indicates either under or over defined thresholds as follows:

- overThreshold - utilization has exceeded the configured threshold level.
- underThreshold - utilization has returned to below the configured threshold abatement level.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Receive utilization is $UtilizationState at $UtilizationPercent% .
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Send utilization is $UtilizationState at $UtilizationPercent% .

Message Substitution Variables:

CommonNodeSignalingPointLinksetLink

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
Substitution variables for Link related data.	
LinksetName	The name of the Linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetLocalPointCode	The local point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
LinksetAdjacentPointCode	The adjacent point code specification for this linkset from the MWTM object database or from the raw trap PDU if the Linkset could not be resolved in the MWTM object database.
SLC	The SLC id value of the link extracted from the trap PDU.
UtilizationState	The current threshold position either overThreshold or underThreshold.
UtilizationPercent	The current percentage of utilization for the link based on the capacity and bytes sent or received.
SequenceNumber	For the ciscoGspLinkRcvdUtilChange and ciscoGspLinkSentUtilChange traps only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the utilization state is 'underThreshold' then no action is necessary.
- If the utilization state is 'overThreshold' then you may want to add few links or look at rerouting some traffic across other links. At certain points in time the UtilizationPercent may exceed 100% due to timing considerations during utilization calculation. UtilizationPercent's of 999% can most often be ignored unless it occurs excessively. UtilizationPercent can also exceed 100% when the planned capacity

specified on the ITP router for a link is specified as less than the actual capacity of the link.

- If the traffic in the links exceeds specified values, it can indicate that ITP may not be able to handle traffic if mate fails.

Diagnostic Commands:

To display information about the current state of the links in the linkset use command:

show cs7 [instance-number] linkset [*ls-name* statistics | state | utilization]

ls-name	(Optional) Linkset name. Displays information for this particular linkset.
statistics	(Optional) Displays link usage statistics.
state	(Optional) Displays MTP3 states for link.
utilization	(Optional) Displays link utilization statistics.

Go Top

SECTION 8.7

Trap: cItpRouteStateChange and ciscoGrtDestStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RouteDestState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became Accessible.	RouteDestState	ITP
RouteDestState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became Inaccessible.	RouteDestState	ITP
RouteDestState	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became Restricted.	RouteDestState	ITP
RouteDestState	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became $RouteDestinationState.	RouteDestState	ITP
RouteDestState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $cgrtDestDisplay_cgspInstNetwork/$cgrtDestDisplay_cgrtRouteDpc/$cgrtDestDisplay_cgrtRouteMask became accessible.	RouteDestState	ITP
RouteDestState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $cgrtDestDisplay_cgspInstNetwork/$cgrtDestDisplay_cgrtRouteDpc/$cgrtDestDisplay_cgrtRouteMask became inaccessible.	RouteDestState	ITP
RouteDestState	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $cgrtDestDisplay_cgspInstNetwork/$cgrtDestDisplay_cgrtRouteDpc/$cgrtDestDisplay_cgrtRouteMask became restricted.	RouteDestState	ITP
RouteDestState	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliCode) $SpDisplayName:$cgrtDestDisplay_cgspInstNetwork - Destination $cgrtDestDisplay_cgspInstNetwork/$cgrtDestDisplay/$cgrtDestDisplay_cgrtRouteMask became $cgrtDestStatus.	RouteDestState	ITP
RouteDestState	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became Accessible.	RouteDestState	ITP
RouteDestState	Poll	Alarm	Yes	Major	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became Inaccessible.	RouteDestState	ITP
RouteDestState	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became Restricted.	RouteDestState	ITP

Description:

These traps provide information when a destination changes states. Large number of destinations prevent generating a single trap per state change. Destination state changes will be sent in bundles and suppressed in certain conditions. Because of the way these traps are designed they can be represented by 1 or more MWTM events. The first event will show whether or not destination state changes were suppressed. The 'NotifInfoSuppressed' key will indicate this state as follows:

- True - Indicates that the device has suppressed the sending of notifications for the remainder of the time interval.
- False- Indicates that the device has not suppressed the sending of notifications in the current time interval.

The second and subsequent events that can be generated will indicate which destinations changed state and what the new 'RouteDestinationState' is as follows:

- Unknown - A destination state of unknown occurs when the destination is a summary route. Unknown state is presented to indicate the protocols do not exchange state information for summary routes in certain configurations.
- Accessible - The destination can be reached by one or more routes specified for the destination. When summary routing is enabled, a destination status will also depend on route table entries that specify less specific matches.
- Inaccessible - Destination can not be reached by any route known to this signaling point.
- Restricted - Traffic has been restricted from being sent to the destination. The restricted state indicates that the primary route for the destination is unavailable or that it is impacted by some network event or failure of resource.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Had destination state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - No destination state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became $RouteDestinationState.

Message Substitution Variables:

CommonNodeSignalingPoint

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
NotifInfoSuppressed	A flag indicating if destination state changes were suppressed, extracted from the trap PDU.
RouteStateChangeCount	The number of destination state changes reflected in this trap, extracted from the trap PDU.
RouteDestinationState	The current state of the destination, extracted from the trap PDU.
RouteTableName	The route table that contains the definition for this destination, extracted from the trap PDU. For the cItpRouteStateChange trap this is the actual route table name and for the ciscoGrtDestStateChange trap this is the ITP network instance name.
RouteDPC	The destination point code specified for the destination, extracted from the trap PDU.
RouteMask	The route mask specified for the RouteDPC, extracted from the trap PDU.
RouteCongestionState	The route congestion state value is valid only for the ciscoGrtDestStateChange trap. One of None, Low, High, or Very High.
SequenceNumber	For the ciscoGrtDestStateChange trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the NotifInfoSuppressed flag indicates that destination changes have been suppressed. It may be necessary to suppress the sending of notifications when a large number destinations change state, due the failure of some common resource. The number of notifications can be controlled by specifying values for NotifWindowTime and NotifMaxPerWindow objects. When the number of destination state changes exceed the specified value the last notification will indicate that notifications are suppressed for the remainder of the window.
- If the RouteState indicates that destinations have become unavailable or restricted you may want to investigate linkset unavailability as the cause.

Diagnostic Commands:

To display the list of routes for a given destination-point-code, use the show cs7 route in EXEC command mode.

show cs7 [*instance-number*] route [*pc* [summary-routes]] [brief | detailed]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
pc	Point code
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a detailed form of the output.

Additional Information:

The following configuration options effect the route and destination status information:

summary-routing-exception

The summary-routing-exception configuration option indicates whether to use the summary route when the fully qualified route is not available. By default the summary-routing-exception option is off and summary route can be used to route MTP3 messages. In a case, when a summary route is available and fully qualified route is unavailable the destination status for the fully qualified route will be restricted rather than unavailable. When summary-routing-exception option is enabled the destination status for the fully qualified route will be unavailable.

max-dynamic-routes

The max-dynamic-routes configuration option defines the maximum number of dynamic routes allowed for the signaling point. If the limit is reached the status of some routes will not reflect the information reflected in the MTP3 management packets.

national-options TFR

This option applies only to ITU and china variants and indicates whether transfer restricted MTP3 management messages will be exchanged between signaling points. When this options is enabled route and destination statuses can display the restricted state.

Note: Changing any of the global configuration options on an operational box will not update all route and destination statuses. Routing behavior will change correctly, although it might not match what would be indicated by some destination statuses. These options are intended to be a one-time configuration before the box is put in service.

Go Top

SECTION 8.8

Trap: ciscoGrtRouteTableLoad

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RouteTableLoad	Trap	Alarm	Yes	Informational	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - Route table $RouteTableName load in progress from $RouteTableUrl.	RouteTableLoad	ITP
RouteTableLoad	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - Route table $RouteTableName load complete from $RouteTableUrl.	RouteTableLoad	ITP
RouteTableLoad	Trap	Alarm	Yes	Minor	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - Route table $RouteTableName load from $RouteTableUrl completed with errors.	RouteTableLoad	ITP
RouteTableLoad	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - Route table $RouteTableName load from $RouteTableUrl failed.	RouteTableLoad	ITP

Description:

The ciscoGrtRouteTableLoad trap is generated whenever a load operation is started or completes for an ITP Route table. The value of TableLoadState indicates the current state of the load process. Possible values of TableLoadState include:

- LoadInProgress - load request is active.
- LoadComplete - load request complete without errors.
- LoadCompleteWithErrors - Load request completed with some type of errors that prevented the adding of one or more entries.
- LoadFailed - Load request failed.

Default Message:

- $NodeDisplayName ($NodeCliliCode) $SpDisplayName - Route table $RouteTableName load in progress from $RouteTableUrl.
- $NodeDisplayName ($NodeCliliCode) $SpDisplayName - Route table $RouteTableName load complete from $RouteTableUrl.
- $NodeDisplayName ($NodeCliliCode) $SpDisplayName - Route table $RouteTableName load from $RouteTableUrl completed with errors.
- $NodeDisplayName ($NodeCliliCode) $SpDisplayName - Route table $RouteTableName load from $RouteTableUrl failed.

Message Substitution Variables:

CommonNodeSignalingPoint

Substitution variables common to all traps.
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.

Substitution variables for SignalingPoint related data.	
RouteTableName	The destination name of the route table being loaded.
RouteTableUrl	The source of the route table being loaded.
TableLoadState	The state of the load process being performed. One of LoadInProgress, LoadComplete, LoadCompleteWithErrors, or LoadFailed.
SequenceNumber	SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the state of the table load is LoadFailed it may indicate that an incorrect file was specified or the file contains errors or it may be placed on an incorrect device.
- If the state of the table load is LoadCompleteWithErrors or LoadFailed it can indicate that the traffic to destination may be impacted or failed.
- You can also check the syslog on the ITP router for further diagnostic information.

Diagnostic Commands:

To collect additional information for failure use the following commands:

show run

show flash:

show disk0:

Go Top

SECTION 8.9

Trap: cItpSccpGttMapStateChange and ciscoGsccpGttMapStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GttMapState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Map PointCode/subsystem $MapPointCode/$MapSubSystem is Allowed.	GttMapState	ITP
GttMapState	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Map PointCode/subsystem $MapPointCode/$MapSubSystem is Prohibited.	GttMapState	ITP
GttMapState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Map PointCode/subsystem $MapPointCode/$MapSubSystem is Allowed.	GttMapState	ITP
GttMapState	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Map PointCode/subsystem $MapPointCode/$MapSubSystem is Prohibited.	GttMapState	ITP

Description:

These traps provide information when a mated application subsystem changes to a new state. The 'MapSsState' key will indicate this state as follows:

- Allowed - The mated application is allowed.
- Prohibited - The mated application is prohibited.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Map PointCode/subsystem $MapPointCode/$MapSubSystem is Allowed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Map PointCode/subsystem $MapPointCode/$MapSubSystem is Prohibited.

Message Substitution Variables:

CommonNodeSignalingPoint

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
MapPointCode	The point code for GTT MAP entry.

MapSubSystem	The subsystem number (SSN) for GTT MAP entry.
MapSsState	The GTT MAP subsystem status.
SequenceNumber	For the ciscoGsccpGttMapStateChange trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the state is 'Initial' then it indicates that HSRP is not running. This state is entered via a configuration change or when an interface first comes up.

Diagnostic Commands:

1. To display cs7 GTT map entries, use the show cs7 gtt map privileged EXEC command.

show cs7 [*instance-number*] gtt map [ppc *pc* [SSN *ssn*]] [status]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
ppc	Specifies a primary point code.
pc	Primary SS7 point code, in the form zone.region.sp.
SSN	Specifies a subsystem number.
ssn	Subsystem number in the range 2 through 255.
status	(Optional) Display the status of the subsystems.

2. Use "show cs7 route" if point code status is not available. Display list of routes for a given destination-point-code.

show cs7 [*instance-number*] route [*pc* [summary-routes]] [brief | detailed]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
pc	Point code
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a comprehensive information with the breakdown of aggregated status into the linkset status and the non-adjacent status.

Go Top

SECTION 8.10

Trap: ciscoGsccpGttLoadTable

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GttTableLoad	Trap	Alarm	Yes	Informational	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Gtt table load in progress from $GttTableUrl.	GttTableLoad	ITP
GttTableLoad	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Gtt table load complete from $GttTableUrl.	GttTableLoad	ITP
GttTableLoad	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Gtt table load from $GttTableUrl completed with errors.	GttTableLoad	ITP
GttTableLoad	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliCode) $SpDisplayName - Gtt table load from $GttTableUrl failed.	GttTableLoad	ITP

Description:

The ciscoGsccpGttLoadTable trap is generated whenever a load operation is started or completes for an ITPGTT table. The value of TableLoadState indicates the current state of the load process. Possible values of TableLoadState include:

- LoadInProgress - load request is active.
- LoadComplete - load request complete without errors.
- LoadCompleteWithErrors - Load request completed with some type of errors that prevented the adding of one or more entries.
- LoadFailed - Load request failed.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Gtt table load in progress from $GttTableUrl.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Gtt table load complete from $GttTableUrl.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Gtt table load from $GttTableUrl completed with errors.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Gtt table load from $GttTableUrl failed.

Message Substitution Variables:

CommonNodeSignalingPoint

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
GttTableUrl	The source of the Gtt table being loaded.
TableLoadState	The state of the load process being performed. One of LoadInProgress, LoadComplete, LoadCompleteWithErrors, or LoadFailed.
SequenceNumber	SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the state of the table load is LoadFailed it may indicate that an incorrect file was specified or the file contains errors or it may be placed on an incorrect device.
- If the state of the table load is LoadCompleteWithErrors or LoadFailed it can indicate that the traffic to global title translation may be impacted or failed.
- You can also check the syslog on the ITP router for further diagnostic information.

Diagnostic Commands:

To collect additional information for failure use the following commands:

show run

show flash:

show disk0:

Go Top

SECTION 8.11

Trap: ciscoGsccpGttErrors

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GttErrors	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - GTT errors have cleared.	GttErrors	ITP
GttErrors	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - GTT errors have occurred: SelectorNotFound=$SelectorNotFound, IncorrectFormat=$IncorrectFormat, GtaNotFound=$GtaNotFound, HopViolation=$HopViolation, MapNotFound=$MapNotFound, UnequipedSS=$UnequipedSS, SccpUnavailable=$SccpUnavailable, DpcUnavailable=$DpcUnavailable, SsUnavailable=$SsUnavailable, DpcCongested=$DpcCongested, SsCongested=$SsCongested, RouteFailure=$RouteFailure, SccpUnqualified=$SccpUnqualified	GttErrors	ITP

Description:

This notification is generated whenever any global title error isencountered
in last interval specified by the cgsccpGttErrorPeriod and the
cgsccpInstErrorIndicator
will be set to true. The notification will also be generated when
errors
have abated. The notification is generated after the number of recovery
intervals
as specified by the cgsccpGttErrorRecoveryCount object has passed
without
any global title errors.

Default Messages:

- NodeDisplayName ($NodeClliCode) $SpDisplayName - GTT errors have occurred:
  SelectorNotFound=$SelectorNotFound, IncorrectFormat=$IncorrectFormat,
  GtaNotFound=$GtaNotFound,
  HopViolation=$HopViolation, MapNotFound=$MapNotFound,
  UnequipedSS=$UnequipedSS,
  SccpUnavailable=$SccpUnavailable, DpcUnavailable=$DpcUnavailable,
  SsUnavailable=$SsUnavailable,
  DpcCongested=$DpcCongested, SsCongested=$SsCongested,
  RouteFailure=$RouteFailure,
  SccpUnqualified=$SccpUnqualified.

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - GTT errors have cleared.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.
SignalingPoint	Substitution variables for SignalingPoint related data.
ErrorIndicator	Indicates whether global title translation errors have occurred in last interval
SelectorNotFound	Counter for the number of times a translation was requested for a combination of Translation Type
IncorrectFormat	Counter for the number of times an invalid Global Title format is found while performing the global title translation
GtaNotFound	Counter for the number of times a global title translation was required and a selector was not found
HopViolation	Counter for the number of times a hop count violation is found in the MSU
MapNotFound	Counter for the number of times a global title translation is successful to a certain PC/SSN but it was not found in the GTT Mated Application table
UnequipedSS	Counter for the number of times a global title translation could not be performed due to an unequipped subsystem (SS)
SccpUnavailable	Counter for the number of times a SCCP is unavailable at the GTT Mated Application
DpcUnavailable	Counter for the number of times a point code is unavailable at the GTT Mated Application
SsUnavailable	Counter for the number of times a subsystem is unavailable at the GTT Mated Application
DpcCongested	Counter for the number of times a point code is congested at the GTT Mated Application
SsCongested	Counter for the number of times a subsystem is congested at the GTT Mated Application
RouteFailure	Counter for the number of times a the MTP3 layer failed at the GTT Mated Application
SccpUnqualified	Counter for the number of times a global title translation is unsuccessful and the error type not covered by other specific error types

Operational Information:

- The 'warning' notification is generated whenever any global title error is encountered in last interval (defined by error period on the router).
- The 'cleared' notification is generated whenever the number of contiguous sample windows (as defined on the router) have been error free.

Diagnostic Commands:

1. For route or DPC congestion failures use "show cs7 route" in EXEC command mode. Displays the list of routes for a given destination-point-code.

show cs7 [*instance-number*] route [*pc* [summary-routes]] [brief | detailed]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
pc	Point code
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a comprehensive information with the breakdown of aggregated status into the linkset status and the non-adjacent status.

2. For selector failures use "show cs7 gtt selector" in privileged EXEC command mode. The output can be compared against the error messages in the gtt error log.

show cs7 [instance-number] gtt selector [gti gti] [nai nai] [name selector-name] [np np] [tt tt]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
gti	(Optional) Specifies a global title indicator.
gti	Global title indicator. Valid range is 0 through 4.
nai	(Optional) Specifies a nature of address indicator.
nai	Nature of address indicator.
name	(Optional) CS7 GTT selector name.
name	Selector name.
np	(Optional) Specifies a numbering plan.
np	Numbering plan.
np	(Optional) Specifies a numbering plan.
np	Numbering plan.
tt	(Optional) Specifies a translation type.
tt	Translation type.

3. To display a summary of CS7 GTT/SCCP measurements, use the show cs7 gtt measurements privilegedEXEC command.

show cs7 [instance-number] gtt measurements [app-grp app-grp-name] | [counters] | [map] |[selector [selector]] | [systot] | [line-card [line-card-num]]

app-group	(Optional) Displays measurements kept on a GTT application group basis.
app-grp-name	GTT application group name.
counters	(Optional) Displays Q.752 counters for GTT.
instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
line-card	(Optional) Display measurements kept on a line card basis. The line-card option is available only if MTP3 offload is enabled (only on the Cisco 7500.)
line-card-num	(Optional) Line card number. If line-card-num is not specified, all line-card measurements for all line cards are displayed.
map	(Optional) Displays measurements kept on a GTT MAP basis.
selector	(Optional) Display statistics kept on a GTT selector basis.
selector	(Optional) Display statistics for a specified selector.
systot	(Optional) Displays measurements kept on a system-wide basis.

4. For SsUnavailable use "show cs7 gtt map status" in privileged EXEC command.

show cs7 [*instance-number*] gtt map [ppc *pc* [SSN *ssn*]] [status]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
ppc	Specifies a primary point code.
pc	Primary SS7 point code, in the form zone.region.sp.

SSN	Specifies a subsystem number.
ssn	Subsystem number in the range 2 through 255.
status	(Optional) Display the status of the subsystems.

5. For GTA not found, use "show cs7 gtt gta" in privileged EXEC command.

show cs7 [instance-number] gtt gta selector-name [sgta sgta egta egta]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
selector-name	Selector name
sgta	Specifies a start global title address
sgta	Starting global title address
egta	Specifies an end global title address
egta	Ending global title address.

6. For general GTT troubleshooting use "show cs7 sccp event-history"

show cs7 sccp event-history [event-count]

event-count	<1-1024> Number of events to display.

Go Top

SECTION 8.12

Trap: ciscoGsccpSegReassUnsup

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SCCPMsgDroppedWithErrors	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - SCCP Message dropped due to segmentation or reassembly unsupported or failure Errors : GttErrorReassemblyUnsupported=$cgsccpGttErrorsReassUnsupported, GttErrorReassemblyFailure=$cgsccpGttErrorsReassFailure, GttErrorSegmentationUnsupported=$cgsccpGttErrorsSegUnsupported, GttErrorSegmentationFailure=$cgsccpGttErrorsSegFailure.	SCCPMsgDroppedWithErrors	ITP
SCCPMsgDroppedWithErrors	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Gtt Segmentation or reassembly unsupported or failure Errors have cleared.	SCCPMsgDroppedWithErrors	ITP

Description:

```
This notification is generated initially when a SCCP message        is dropped due to a segmentation or reassembly unsupported
or failure errors in last interval specified by the
cgsccpGttErrorPeriod and the cgsccpInstErrorIndicator will be
set to true.  The notification will also be generated after
the number of recovery intervals as specified by the
cgsccpGttErrorRecoveryCount object has passed without any
segmentation or reassembly unsupported errors.
```

Default Message:

$NodeDisplayName ($NodeClliCode) $SpDisplayName - SCCP Message dropped due to segmentation or reassembly unsupported or failure Errors : GttErrorReassemblyUnsupported=$cgsccpGttErrorsReassUnsupported, GttErrorReassemblyFailure=$cgsccpGttErrorsReassFailure, GttErrorSegmentationUnsupported=$cgsccpGttErrorsSegUnsupported, GttErrorSegmentationFailure=$cgsccpGttErrorsSegFailure.
$NodeDisplayName ($NodeClliCode) $SpDisplayName - Gtt Segmentation or reassembly unsupported or failure Errors have cleared.

Message Substitution Variables:

SignalingPoint

Common	Substitution variables common to all traps.

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
Substitution variables for SignalingPoint related data.	
MapPointCode	The point code for GTT MAP entry.
MapSubSystem	The subsystem number (SSN) for GTT MAP entry.
SequenceNumber	For the ciscoGsccpSegReassUnsup trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.
cgsccpInstErrorIndicator	This object indicates whether global title translation errors have occurred in last interval specified by the cgsccpGttErrorPeriod object. Represents a boolean value.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgsccpGttErrorsReassUnsupported	This counter is incremented every time when the incoming SCCP message needs to be dropped due to the unsupported reassembly feature. This counter is derived from cgsccpInstReassUnsup object.
cgsccpGttErrorsReassFailure	This counter is incremented every time when the incoming SCCP message needs to be dropped due to the reassembly failure. This counter is derived from cgsccpInstReassFail object.
cgsccpGttErrorsSegUnsupported	This counter is incremented every time when either SCCP message from a remote node or local SCCP stack needs to be dropped due to the unsupported segmentation feature. This counter is derived from cgsccpInstSegUnsup object.
cgsccpGttErrorsSegFailure	This counter is incremented every time when either SCCP message from a remote node or local SCCP stack needs to be dropped due to the segmentation failure. This counter is derived from cgsccpInstSegFail object.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.

Go Top

SECTION 8.13

Trap: ciscoGsccpLocalSsStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GttLocalSsState	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliiCode) - Local subsystem $cgsccpLocalDisplaySS state change is Prohibited.	GttLocalSsState	ITP
GttLocalSsState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliiCode) - Local subsystem $cgsccpLocalDisplaySS state change is allowed.	GttLocalSsState	ITP

Description:

```
The notification generated when a local application subsystem        changes to a new state.  The subsystem number and the latest
subsystem state will be provided in this notification.
```

Default Message:

$NodeDisplayName ($NodeCliliCode) - Local subsystem $cgsccpLocalDisplaySS state change is Prohibited.
$NodeDisplayName ($NodeCliliCode) - Local subsystem $cgsccpLocalDisplaySS state change is allowed.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
SequenceNumber	For the ciscoGsccpLocalSsStateChange trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.
cgsccpLocalSsStatus	Local subsystem status. The list of SCCP GTT Mated App subsystem status 'allowed' : The mated application is allowed 'prohibited' : The mated application is prohibited.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgsccpLocalDisplaySS	Local subsystem in display format.

Go Top

SECTION 8.14

Trap: ciscoGsccpRmtCongestion

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RemoteSCCPCongestion	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- The remote SCCP component has congestion level 1.	RemoteSCCPCongestion	ITP
RemoteSCCPCongestion	Trap	Alarm	Yes	Minor	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- The remote SCCP component has congestion level 2.	RemoteSCCPCongestion	ITP
RemoteSCCPCongestion	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- The remote SCCP component has congestion level 3.	RemoteSCCPCongestion	ITP
RemoteSCCPCongestion	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- The remote SCCP component has no congestion.	RemoteSCCPCongestion	ITP

Description:

```
This notification is generated initially when congestion is        experienced in the remote SCCP component for the first time in
last interval specified by the cgsccpGttErrorPeriod.  The
notification is generated after the number of recovery intervals
as specified by the cgsccpGttErrorRecoveryCount object has
passed without any congestion errors and total number of local
congestion observed for different congestion levels at the end
of the interval along with the latest known congestion status
for that remote signalling point will be provided.
```

Default Message:

$NodeDisplayName ($NodeCllicode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- The remote SCCP component has congestion level 1.
$NodeDisplayName ($NodeCllicode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- The remote SCCP component has congestion level 2.
$NodeDisplayName ($NodeCllicode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- The remote SCCP component has congestion level 3.
$NodeDisplayName ($NodeCllicode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- The remote SCCP component has no congestion.

Message Substitution Variables:

SignalingPoint

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
Substitution variables for SignalingPoint related data.	
MapPointCode	The point code for GTT MAP entry.
MapSubSystem	The subsystem number (SSN) for GTT MAP entry.
SequenceNumber	For the ciscoGsccpRmtCongestion trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.
cgsccpGttMapCongStatus	The status of congestion level for this MAP point code. The list of SCCP GTT Mated App congestion status 'NotCong' : The point code not congested 'CongLevel1' : The congestion level 1 'CongLevel2' : The congestion level 2 'CongLevel3' : The congestion level 3.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgsccpGttMapDisplayPC	The MAP point code in display format.
cgsccpGttMapCongLvl1	This counter is incremented every time a congestion of level 1 is experienced by the remote Signalling point corresponding to this MAP entry.
cgsccpGttMapCongLvl2	This counter is incremented every time a congestion of level 2 is experienced by the remote Signalling point corresponding to this MAP entry.
cgsccpGttMapCongLvl3	This counter is incremented every time a congestion of level 3 is experienced by the remote Signalling point corresponding to this MAP entry.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.
cgsccpGttMapSsn	The subsystem number (SSN) for GTT MAP entry.

cgsccpGttMapPc	The point code for GTT MAP entry.

Go Top

SECTION 8.15

Trap: ciscoItpXuaAspStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApplicationServerProcessAssociationState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliCode) $SpDisplayName - ASP $ASPName in AS $ASName state is Active.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Trap	Alarm	Yes	Critical	$NodeDisplayName ($NodeCliCode) $SpDisplayName - ASP $ASPName in AS $ASName state is Down.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Trap	Alarm	Yes	Minor	$NodeDisplayName ($NodeCliCode) $SpDisplayName - ASP $ASPName in AS $ASName state is Inactive.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliCode) $SpDisplayName - ASP $ASPName in AS $ASName state is Undefined.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Normal	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName added in state Active/ActiveReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Event	Yes	Normal	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to Active/ActiveReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Normal	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to Available/AvailableReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Warning	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName added in state Shutdown/ShutdownReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Major	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName added in state Inactive/InactiveReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Event	Yes	Warning	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName added in state Warning/WarningReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Critical	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName added in state Down/DownReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Minor	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName added in state Pending/PendingReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Warning	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to Shutdown/ShutdownReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Major	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to Inactive/InactiveReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Event	Yes	Warning	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to Warning/WarningReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Critical	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to Down/DownReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Event	Yes	Major	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to Unknown/UnknownReason.	ApplicationServerProcessAssociationState	ITP

ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Minor	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to Pending/PendingReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Major	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName added in state Blocked/BlockedReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Event	Yes	Informational	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName added in state $ASPAState/$ASPAStateReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Alarm	Yes	Major	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to Blocked/BlockedReason.	ApplicationServerProcessAssociationState	ITP
ApplicationServerProcessAssociationState	Poll	Event	Yes	Informational	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName changed state from $ASPALastState to $ASPAState/$ASPAStateReason.	ApplicationServerProcessAssociationState	ITP

Description:

This trap provides information when an ASP (Application Server Process) changes to a new state. The 'AspState' key will indicate this state as follows:

- Down - The remote peer at the ASP is unavailable and/or the related SCTP association is down. Initially all ASPs will be in this state.
- Inactive - The remote peer at the ASP is available (and the related SCTP association is up) but application traffic is stopped. In this state the ASP should not be sent any DATA or SNMM messages for the AS for which the ASP is inactive.
- Active - The remote peer at the ASP is available and application traffic is active.
- Undefined - The state of the remote peer at the ASP is not known or undefined.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - ASP $ASPName in AS $ASName state is $AspState.

Message Substitution Variables:

CommonNodeSignalingPointApplicationServerApplicationServerProcessApplicationServerProcessAssociation

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the SGM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
Substitution variables for ApplicationServer related data.	
Substitution variables for ApplicationServerProcess related data.	
Substitution variables for ApplicationServerProcessAssociation related data.	
AspState	The state of the ASP. One of Down, Inactive, Active, or Undefined.

Operational Information:

- If the state is Active, no action is necessary.
- If the state is Down, determine if the IP address or port configuration match between the local and the remote peer.
- An ASP can remain in Inactive state. Depending on the traffic mode of the AS the ASPs belonging to that AS can change between active to inactive states.
- If the state of the ASP is 'Undefined' it indicates that an attempt to determine the state of the ASP failed. At this state the ASP cannot be used for application traffic. You may want to check with the ITP administrator and analyze this ASP for faults.

Diagnostic Commands:

To display ASP information, use the 'show cs7 asp' command in privileged EXEC mode.

show cs7 [*instance-number*] asp [m3ua | sua | all | name *asp-name* | asname *as-name*] [statistics [detail] | bindings | detail | event-history]

instance-number	(Optional) Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
m3ua	(Optional) Filter on M3UA.
sua	(Optional) Filter on SUA.
all	Display all ASPs. (Default)
name	(Optional) Filter on ASP name.
asp-name	(Optional) ASP name.
asname	(Optional) Filter on AS name.
statistics	(Optional) Display ASP statistics.
bindings	(Optional) Display ASP bindings
detail	(Optional) Display in detail format.
event-history	(Optional) Display ASP history.

Go Top

SECTION 8.16

Trap: ciscoItpXuaSgmStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SgmpAssociationState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliCode) - SGMP $SGMPName state is Active.	SgmpAssociationState	ITP
SgmpAssociationState	Trap	Alarm	Yes	Critical	$NodeDisplayName ($NodeCliCode) - SGMP $SGMPName state is Down.	SgmpAssociationState	ITP
SgmpAssociationState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliCode) - SGMP $SGMPName state is Inactive.	SgmpAssociationState	ITP
SgmpAssociationState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliCode) - SGMP $SGMPName state is Undefined.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Alarm	Yes	Normal	SGMP $NodeDisplayName/$SGMPName added in state Active/ActiveReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Event	Yes	Normal	SGMP $NodeDisplayName/$SGMPName changed state from $SGMPLastState to Active/ActiveReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Alarm	Yes	Normal	SGMP $NodeDisplayName/$SGMPName changed state from $SGMPLastState to Available/AvailableReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Alarm	Yes	Major	SGMP $NodeDisplayName/$SGMPName added in state Inactive/InactiveReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Alarm	Yes	Critical	SGMP $NodeDisplayName/$SGMPName added in state Down/DownReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Event	Yes	Warning	SGMP $NodeDisplayName/$SGMPName added in state Warning/WarningReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Alarm	Yes	Warning	SGMP $NodeDisplayName/$SGMPName added in state Shutdown/ShutdownReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Event	Yes	Informational	SGMP $NodeDisplayName/$SGMPName added in state $SGMPState/$SGMPStateReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Alarm	Yes	Major	SGMP $NodeDisplayName/$SGMPName changed state from $SGMPLastState to Inactive/InactiveReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Alarm	Yes	Critical	SGMP $NodeDisplayName/$SGMPName changed state from $SGMPLastState to Down/DownReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Event	Yes	Warning	SGMP $NodeDisplayName/$SGMPName changed state from $SGMPLastState to Warning/WarningReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Alarm	Yes	Warning	SGMP $NodeDisplayName/$SGMPName changed state from $SGMPLastState to Shutdown/ShutdownReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Event	Yes	Major	SGMP $NodeDisplayName/$SGMPName changed state from $SGMPLastState to Unknown/UnknownReason.	SgmpAssociationState	ITP
SgmpAssociationState	Poll	Event	Yes	Informational	SGMP $NodeDisplayName/$SGMPName changed state from $SGMPLastState to $SGMPState/$SGMPStateReason.	SgmpAssociationState	ITP

Description:

This trap provides information when a SG Mate (Signaling Gateway Mate) changes to a new state. The 'SgmpState' key will indicate this state as follows:

- Inactive - The remote peer at the SG Mate is unavailable.
- Active - The remote peer at the SG Mate is available and application traffic is active.
- Undefined - The state of the remote peer at the SG Mate is not known or undefined.

Default Message:

$NodeDisplayName ($NodeCliliCode) - SGMP $SGMPName state is $SgmpState.

Message Substitution Variables:

CommonNodeSignaling Gateway Mate

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingGatewayMatedPairAssociation related data.	
SgmpState	The state of the SG Mate. One of Down, Inactive, Active, or Undefined.

Operational Information:

- If the state is Active, no action is necessary.
- If the state is Inactive, determine if the IP address or port configuration match between the local and the remote peer.
- If the state of the SG Mate is 'Undefined' it indicates that an attempt to determine the state of the SG Mate failed. At this state the SG Mate cannot be used for application traffic. You may want to check with the ITP administrator and analyze this SG Mate for faults.

Diagnostic Commands:

To determine the status of the mated pair use the following show command.

show cs7 [*instance-number*] mated-sg [detail | statistics]

instance-number	(Optional) Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
detail	(Optional) Displays in detail format.
statistics	(Optional) Displays mated-sg statistics

Go Top

SECTION 8.17

Trap: ciscoItpXuaAsStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApplicationServerState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - AS $ASName state is Active.	ApplicationServerState	ITP
ApplicationServerState	Trap	Alarm	Yes	Critical	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - AS $ASName state is Down.	ApplicationServerState	ITP
ApplicationServerState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - AS $ASName state is Inactive.	ApplicationServerState	ITP
ApplicationServerState	Trap	Alarm	Yes	Minor	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - AS $ASName state is Pending.	ApplicationServerState	ITP
ApplicationServerState	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliliCode) $SpDisplayName - AS $ASName state is Undefined.	ApplicationServerState	ITP
ApplicationServerState	Poll	Alarm	Yes	Normal	AS $NodeDisplayName/$SpDisplayName/$ASName added in state Active/ActiveReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Alarm	Yes	Normal	AS $NodeDisplayName/$SpDisplayName/$ASName changed state from $ASLastState to Active/ActiveReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Alarm	Yes	Major	AS $NodeDisplayName/$SpDisplayName/$ASName added in state Inactive/InactiveReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Alarm	Yes	Critical	AS $NodeDisplayName/$SpDisplayName/$ASName added in state Down/DownReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Alarm	Yes	Minor	AS $NodeDisplayName/$SpDisplayName/$ASName added in state Pending/PendingReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Event	Yes	Warning	AS $NodeDisplayName/$SpDisplayName/$ASName added in state Warning/WarningReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Alarm	Yes	Warning	AS $NodeDisplayName/$SpDisplayName/$ASName added in state Shutdown/ShutdownReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Event	Yes	Informational	AS $NodeDisplayName/$SpDisplayName/$ASName added in state $ASState/$ASStateReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Alarm	Yes	Major	AS $NodeDisplayName/$SpDisplayName/$ASName changed state from $ASLastState to Inactive/InactiveReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Alarm	Yes	Critical	AS $NodeDisplayName/$SpDisplayName/$ASName changed state from $ASLastState to Down/DownReason.	ApplicationServerState	ITP
					AS $NodeDisplayName/$SpDisplayName/$ASName changed state from $ASLastState to		

ApplicationServerState	Poll	Alarm	Yes	Minor	Pending/PendingReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Event	Yes	Warning	AS $NodeDisplayName/$SpDisplayName/$ASName changed state from $ASLastState to Warning/WarningReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Alarm	Yes	Warning	AS $NodeDisplayName/$SpDisplayName/$ASName changed state from $ASLastState to Shutdown/ShutdownReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Event	Yes	Major	AS $NodeDisplayName/$SpDisplayName/$ASName changed state from $ASLastState to Unknown/UnknownReason.	ApplicationServerState	ITP
ApplicationServerState	Poll	Event	Yes	Informational	AS $NodeDisplayName/$SpDisplayName/$ASName changed state from $ASLastState to $ASState/$ASStateReason.	ApplicationServerState	ITP

Description:

This trap provides information when an AS (Application Server) changes to a new state. The 'AsState' key will indicate this state as follows:

- Down - The AS is unavailable. This state implies that all ASPs that are serving this AS are in the 'down' state. Initially the AS will be in this state.
- Inactive - The AS is available but no application traffic is active (i.e., one or more ASPs are in the inactive state, but none in the active state).
- Active - The AS is available and application traffic is active. This state implies that at least one ASP is in the active state.
- Pending - An active ASP has transitioned to inactive or down and it was the last remaining active ASP serving the AS. Depending on the recovery timer and an ASP becoming active this AS moves to Active, Inactive, or Down state.
- Undefined - The AS state is not known or undefined.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - AS $ASName state is $AsState.

Message Substitution Variables:

CommonNodeSignalingPointApplicationServer

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the SGM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
Substitution variables for ApplicationServer related data.	
AsState	The state of the AS. One of Down, Inactive, Active, Pending, or Undefined.

Operational Information:

- If the state is Active, no action is necessary.
- If the state of the AS is 'Down' then check the status of the ASPs in the AS. Check if IP address or port configuration of the ASPs match between the local and the remote peer. You can also check the IP routing between the local and the remote ASPs. A 'Down' state may also be due to an error occurred while polling the Node that this AS belongs to.
- If the state of the AS is 'Inactive' then check the status of the ASPs in the AS. The ASPs are in inactive state, depending on the traffic mode of the AS. As the traffic mode changes the state of the ASPs change from inactive to active.
- If the state of the AS is 'Pending' then check the status of the ASPs in the AS.
- If the state of the AS is 'Undefined' it indicates that an attempt to determine the state of the AS failed. At this state the AS cannot be used for application traffic. You may want to check with the ITP administrator and analyze this AS for faults.

Diagnostic Commands:

To display AS information, use the show cs7 as privileged EXEC command.

```
show cs7 [instance-number] as [[m3ua [include-gtt | exclude-gtt | only-gtt]]        | [sua [include-gtt | exclude-gtt | only-gtt]]
        | [all [include-gtt | exclude-gtt | only-gtt]]
        | [name as-name]] [operational | active | all)]
        [statistics | detail | brief]
```

(Optional) Specifies the instance. The valid range is 0 through 7.

instance-number	The default instance is instance 0.
m3ua	(Optional) Filter on M3UA.
sua	(Optional) Filter on SUA.
all	Display all ASs. (Default)
include-gtt	(Optional) Include ASs with GTT routing keys. (Default)
exclude-gtt	(Optional) Exclude ASs with GTT routing keys.
only-gtt	(Optional) Display only ASs with GTT routing keys.
name	(Optional) Filter on AS name.
as-name	(Optional) AS name.
operational	(Optional) Display operational ASs. (non-shut state)
active	(Optional) Display only active AS
statistics	(Optional) Display AS statistics.
detail	(Optional) Display AS info in detail format.
brief	(Optional) Display AS info in brief format (Default).

Go Top

SECTION 8.18

Trap: ciscoItpXuaAspCongChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ASPACongestionChange	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) - ASP $ASPName congestion level is None.	ASPACongestionChange	ITP
ASPACongestionChange	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) - ASP $ASPName congestion level is Congestion Level 1.	ASPACongestionChange	ITP
ASPACongestionChange	Trap	Alarm	Yes	Minor	$NodeDisplayName ($NodeClliCode) - ASP $ASPName congestion level is Congestion Level 2.	ASPACongestionChange	ITP
ASPACongestionChange	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeClliCode) - ASP $ASPName congestion level is Congestion Level 3.	ASPACongestionChange	ITP
ASPACongestionChange	Trap	Alarm	Yes	Critical	$NodeDisplayName ($NodeClliCode) - ASP $ASPName congestion level is Congestion Level 4.	ASPACongestionChange	ITP
ASPACongestionChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: congestion level is None.	ASPACongestionChange	ITP
ASPACongestionChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: congestion level is Congestion Level 1.	ASPACongestionChange	ITP
ASPACongestionChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: congestion level is Congestion Level 2.	ASPACongestionChange	ITP
ASPACongestionChange	Poll	Alarm	Yes	Minor	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: congestion level is Congestion Level 3.	ASPACongestionChange	ITP
ASPACongestionChange	Poll	Alarm	Yes	Minor	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: congestion level is Congestion Level 4.	ASPACongestionChange	ITP

Description:

This trap provides information when an ASP (Application Server Process) changes to a new congestion level. The 'CongestionState' key will indicate this state as follows:

- None - ASP is not congested.
- Level 1 - Incremental congestion indicator.
- Level 2 - Incremental congestion indicator.
- Level 3 - Incremental congestion indicator.
- Level 4 - Incremental congestion indicator.

Default Message:

- $NodeDisplayName ($NodeClliCode) - ASP $ASPName congestion level is $CongestionState.

Message Substitution Variables:

CommonNodeApplicationServerProcess

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the SGM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for ApplicationServerProcess related data.	
CongestionState	The current congestion level for this ASP. A value of None indicates that the ASP is not congested. The higher numbers indicate the higher levels of congestion. The congestion level is determined from the SCTP congestion indication and the SCON level received from the ASP.

Operational Information:

- If the level is None. no action is necessary.
- If the level is 1 to 4 it may indicate the application is unable to process the current traffic rate or it may indicate network congestion. The ability to transfer the MSU can be impacted or the MSU can be discarded at these levels. You may want to offload traffic by adding more hardware.

Diagnostic Commands:

To display ASP information, use the show cs7 asp privileged EXEC command.

show cs7 [*instance-number*] asp [m3ua | sua | all | name *asp-name* | asname *as-name*] [statistics [detail] | bindings | detail | event-history]

instance-number	(Optional) Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
m3ua	(Optional) Filter on M3UA.
sua	(Optional) Filter on SUA.
all	Display all ASPs. (Default)
name	(Optional) Filter on ASP name.
asp-name	(Optional) ASP name.
asname	(Optional) Filter on AS name.
statistics	(Optional) Display ASP statistics.
bindings	(Optional) Display ASP bindings
detail	(Optional) Display in detail format.
event-history	(Optional) Display ASP history.

Go Top

SECTION 8.19

Trap: ciscoItpXuaSgmCongChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SGMPCongestionChange	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliiCode) - SGMP $SGMPName congestion level is None.	SGMPCongestionChange	ITP
SGMPCongestionChange	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliiCode) - SGMP $SGMPName congestion level is Congestion Level 1.	SGMPCongestionChange	ITP
SGMPCongestionChange	Trap	Alarm	Yes	Minor	$NodeDisplayName ($NodeCliiCode) - SGMP $SGMPName congestion level is Congestion Level 2.	SGMPCongestionChange	ITP
SGMPCongestionChange	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeCliiCode) - SGMP $SGMPName congestion level is Congestion Level 3.	SGMPCongestionChange	ITP
SGMPCongestionChange	Trap	Alarm	Yes	Critical	$NodeDisplayName ($NodeCliiCode) - SGMP $SGMPName congestion level is Congestion Level 4.	SGMPCongestionChange	ITP
SGMPCongestionChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeCliiCode) - SGMP $SGMPName: congestion level is None.	SGMPCongestionChange	ITP
SGMPCongestionChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliiCode) - SGMP $SGMPName: congestion level is Congestion Level 1.	SGMPCongestionChange	ITP
SGMPCongestionChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeCliiCode) - SGMP $SGMPName: congestion level is Congestion Level 2.	SGMPCongestionChange	ITP
SGMPCongestionChange	Poll	Alarm	Yes	Minor	$NodeDisplayName ($NodeCliiCode) - SGMP $SGMPName: congestion level is Congestion Level 3.	SGMPCongestionChange	ITP

SGMPCongestionChange	Poll	Alarm	Yes	Minor	$NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: congestion level is Congestion Level 4.	SGMPCongestionChange	ITP

Description:

This trap provides information when an SG Mate (Signaling Gateway Mate) changes to a new congestion level. The 'CongestionState' key will indicate this state as follows:

- None - SG Mate is not congested.
- Level 1 - Incremental congestion indicator.
- Level 2 - Incremental congestion indicator.
- Level 3 - Incremental congestion indicator.
- Level 4 - Incremental congestion indicator.
- Level 5 - Incremental congestion indicator.
- Level 6 - Incremental congestion indicator.
- Level 7 - Incremental congestion indicator.

Default Message:

- $NodeDisplayName ($NodeClliCode) - SGMP $SGMPName congestion level is $CongestionState.

Message Substitution Variables:

CommonNodeSignaling Gateway Mate

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingGatewayMatedPairAssociation related data.	
CongestionState	The current congestion level for this SG Mate. A value of None indicates that the SG Mate is not congested. The higher numbers indicate the higher levels of congestion. The congestion level is determined from the SCTP congestion indication and the SCON level received from the ASP.

Operational Information:

- If the state is 'None' then no action is necessary.
- If the state is at any other Level then it indicates that there is a network congestion. You may want to check for network failure or try to offload traffic.

Diagnostic Commands:

To determine the status of the mated pair use the following show commands.

show cs7 [*instance-number*] mated-sg [detail | statistics]

instance-number	(Optional) Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
detail	(Optional) Displays in detail format.
statistics	(Optional) Displays mated-sg statistics

Go Top

SECTION 8.20

Trap: ciscoMlrTableLoad

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MlrTableLoad	Trap	Alarm	Yes	Informational	$NodeDisplayName ($NodeClliCode) - MLR table load in progress from $MlrTableUrl.	MlrTableLoad	ITP
MlrTableLoad	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) - MLR table load complete from $MlrTableUrl.	MlrTableLoad	ITP
MlrTableLoad	Trap	Alarm	Yes	Minor	$NodeDisplayName ($NodeClliCode) - MLR table load from $MlrTableUrl completed with errors.	MlrTableLoad	ITP
MlrTableLoad	Trap	Alarm	Yes	Major	$NodeDisplayName ($NodeClliCode) - MLR table load from $MlrTableUrl failed.	MlrTableLoad	ITP

Description:

The ciscoMlrTableLoad trap is generated whenever a load operation is started or completes for an ITP MLR address table. The value of TableLoadState indicates the current state of the load process. Possiblevalues of TableLoadState include:

- LoadInProgress - load request is active.
- LoadComplete - load request complete without errors.
- LoadCompleteWithErrors - Load request completed with some type of errors that prevented the adding of one or more entries.
- LoadFailed - Load request failed.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - MLR table load in progress from $MlrTableUrl.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - MLR table load complete from $MlrTableUrl.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - MLR table load from $MlrTableUrl completed with errors.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - MLR table load from $MlrTableUrl failed.

Message Substitution Variables:

CommonNodeSignalingPoint

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
MlrTableUrl	The source of the route table being loaded.
TableLoadState	The state of the load process being performed. One of LoadInProgress, LoadComplete, LoadCompleteWithErrors, or LoadFailed.
SequenceNumber	SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the state of the table load is LoadFailed it may indicate that an incorrect file was specified or the file contains errors or it may be placed on an incorrect device.
- You can also check the syslog on the ITP router for further diagnostic information.

Diagnostic Commands:

To collect additional information for failure use the following commands:

show run

show flash:

show disk0:

Go Top

SECTION 8.21

Trap: ciscoBitsClockSource

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BitsClock	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) - BITS clocking source has switched roles, new role is $SourceRoleCurrent, admin role is $SourceRoleAdmin.	BitsClock	ITP
BitsClock	Trap	Alarm	Yes	Minor	$NodeDisplayName ($NodeClliCode) - BITS clocking source unavailable, internal clock will operate in freerun mode.	BitsClock	ITP
BitsClock	Trap	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) - BITS clocking source unavailable, internal clock will operate in holdover mode.	BitsClock	ITP

Description:

This trap is for Building Integrated Timing Supply(BITS) clockingsources. It is used to generate notifications to indicate when clocking sources change.

Default Message:

$NodeDisplayName ($NodeClliCode) - BITS clocking source has switched roles, new role is $SourceRoleCurrent, admin role is $SourceRoleAdmin.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
PhysicalDescr	A textual description of the physical entity. This object should contain a string which identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.
SourceRoleAdmin	Indicates the role of this clock source as defined by system administrator. Possible values are Primary, Secondary, and Tertiary
SourceRoleCurrent	The current role of BITS clock source. Also, indicates when clock source is unavailable. The 'unavailable' value indicates that the external source of clock signal has failed and indicates that this entry can not serve as clock source. Possible values are Unavailable, Primary, Secondary, and Tertiary.

Operational Information:

- The existence of this trap indicates when BITS clocking sources change and should be investigated by the router administrator.

Diagnostic Commands:

To display details about the configured clocks, the current operational clocks and status information use command:

show network-clocks

Go Top

SECTION 8.22

Trap: ciscoGspIsolation

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SignalingPointIsolation	Trap	Alarm	Yes	Critical	SignalingPoint $NodeDisplayName/$SpDisplayName - signaling point is isolated.	SignalingPointIsolation	ITP
SignalingPointIsolation	Poll	Alarm	Yes	Critical	SignalingPoint $NodeDisplayName/$SpDisplayName - signaling point is isolated.	SignalingPointIsolation	ITP
SignalingPointIsolation	Poll	Alarm	Yes	Normal	SignalingPoint $NodeDisplayName/$SpDisplayName - signaling point is not isolated.	SignalingPointIsolation	ITP

Description:

This notification indicates the instance specified by cgspInstDisplayName and cgspInstDescription has become isolated. All linkset used to connect MTP3 node (instance) are unavailable. Isolation is ended when any linkset supported by this instance reaches the active state.

Default Message:

$NodeDisplayName ($NodeClliCode) $SpDisplayName - signaling point is isolated.
$NodeDisplayName ($NodeClliCode) $SpDisplayName - signaling point is active.

Message Substitution Variables:

Common	Substitution variables common to all traps.

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.
SignalingPoint	Substitution variables for SignalingPoint related data.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional information on the device type.
cgspInstDisplayName	A short identifier for the Signalling point. This value can be set by system administrator or defaults to the local point code formatted as an ASCII string.
cgspInstDescription	A textual description for the Signalling point.

Operational Information:

- This indicates a network problem, communication to the ITP is out of service. You may want to check the underlying interfaces of the all the Linkset for possible causes.

Diagnostic Commands:

1. To display information about the current state of the links in the linkset use command:

show cs7 [instance-number] linkset [*ls-name* statistics | state | utilization]

ls-name	(Optional) Linkset name. Displays information for this particular linkset.
statistics	(Optional) Displays link usage statistics.
state	(Optional) Displays MTP3 states for link.
utilization	(Optional) Displays link utilization statistics.

2. To check the MTP3 restart status of the node use "show cs7" in EXEC command mode.

show cs7

Go Top

SECTION 8.23

Trap: ciscoGrtNoRouteMSUDiscards

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NoRouteMSUDiscards	Trap	Alarm	No	Major	$NodeDisplayName ($NodeClliCode) $SpDisplayName has discarded $cgrtIntervalNoRouteMSUs MSUs in the current monitoring interval due to a route data error.	NoRouteMSUDiscards	ITP

Description:

This notification is generated whenever one or more MSU discards happen due to route data error for a specific signalling point instance in the configured monitoring interval. It will also be sent at the end of the monitoring interval whenever one or more MSUs have been discarded. The notification conforms with Q.752 T5E5.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName has discarded $cgrtIntervalNoRouteMSUs MSUs in the current monitoring interval due to a route data error.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgspInstDisplayName	A short identifier for the Signalling point. This value can be set by system administrator or defaults to the local point code formatted as an ASCII string.
cgrtNoRouteMSUsInterval	Duration elapsed since the start of cgrtNoRouteMSUsNotifWindowTime interval. This duration value can range from 0 upto cgrtNoRouteMSUsNotifWindowTime. For the notifications generated at the end of the interval, this value will be equal to cgrtNoRouteMSUsNotifWindowTime.
cgrtIntervalNoRouteMSUs	Number of MSUs discarded due to routing data error in this specific cgspNoRouteMSUsInterval interval.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.

Operational Information:

Receipt of this trap indicates incorrect routing or a data error, and could indicate a severe problem. The operator should immediately determine the cause. This alarm must be manually cleared.

Go Top

SECTION 8.24

Trap: ciscoGspUPUReceived

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
UserPartUnavailableReceived	Trap	Alarm	No	Informational	$NodeDisplayName ($NodeClliCode) $SpDisplayName has received $cgspIntervalUPUs notifications during the current monitoring interval that MTP3 user part $UserPartName is not available.	UserPartUnavailableReceived	ITP

Description:

The ciscoGspUPUReceived trap is generated by the specified ITP node and instance when it receives a User Part Unavailable Message Signal Unit (UPU MSU) from a remote signalling point for the specified MTP3 user part. It sends this trap when it receives a UPU MSU for the first time within the configured monitoring interval. It will also send the trap at the end of each monitoring interval whenever one or more UPU MSUs have been received within that interval for that user part. It suppresses sending this trap between these two points in time. This notification conforms with Q.752 T5E6.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName has received $cgspIntervalUPUs notifications during the current monitoring interval that MTP3 user part $userPartName is not available.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgspInstUserPartDisplay	The associated instance name and user part information formatted for display.
cgspUPUIntervalDuration	Duration elapsed since the start of the cgspUPUNotifWindowTime interval. This duration value can range from 0 upto cgspUPUNotifWindowTime. For the notifications generated at the end of the interval, this value will be equal to cgspUPUNotifWindowTime.
cgspIntervalUPUs	Number of UPU MSUs received or transmitted during this specific cgspUPUIntervalDuration interval.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.
cgspMtp3SI	The service indicator.

Operational Information:

Receipt of this trap reports that an ITP signalling instance has been notified by a remote signalling point that a specific MTP3 user part (e.g., ISUP or SCCP) is not available. Possible causes include: (1) the signalling point is not equipped for that user part; or (2) the user part is not available on that SP (e.g., because of an outage).
This alarm must be manually cleared.

Go Top

SECTION 8.25

Trap: ciscoGspUPUTransmitted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
UserPartUnavailableTransmitted	Trap	Alarm	No	Informational	$NodeDisplayName ($NodeClliCode) $SpDisplayName has sent $cgspIntervalUPUs notifications during the current monitoring interval to a remote signallnig point that MTP3 user part $UserPartName is not available.	UserPartUnavailableTransmitted	ITP

Description:

The ciscoGspUPUTransmitted trap is generated by the specified ITP node and instance when it transmits a User Part Unavailable Message Signal Unit (UPU MSU) for the specified MTP3 user part to a remote signalling point. It sends this trap for the first time when it transmits the UPU MSU for the first time in the configured monitoring interval. It will also send the trap at the end of each monitoring interval whenever it has transmitted one or more UPU MSUs for the specified user part within that interval. It suppresses sending this trap between these two points in time. This notification conforms with Q.752 T5E7.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName has sent $cgspIntervalUPUs notifications during the current monitoring interval to a remote signalling point that MTP3 user part $userPartName is not available.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgspInstUserPartDisplay	The associated instance name and user part information formatted for display.
cgspUPUIntervalDuration	Duration elapsed since the start of the cgspUPUNotifWindowTime interval. This duration value can range from 0 upto cgspUPUNotifWindowTime. For the notifications generated at the end of the interval, this value will be equal to cgspUPUNotifWindowTime.
cgspIntervalUPUs	Number of UPU MSUs received or transmitted during this specific cgspUPUIntervalDuration interval.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.
cgspMtp3SI	The service indicator.

Operational Information:

Receipt of this trap reports that an ITP signalling instance has notified a remote signalling point that a specific MTP3 user part (e.g., ISUP or SCCP) is not available. Possible causes include: (1) the signalling point is not equipped for that user part; or (2) the user part is not available on that SP (e.g., because of an outage).
This alarm must be manually cleared.

Go Top

SECTION 8.26

Trap: ciscoGspRxCongestionChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkRxCongestionChange	Trap	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Received side link congestion level is abate.	LinkRxCongestionChange	ITP
LinkRxCongestionChange	Trap	Alarm	Yes	Minor	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: Received side link congestion level is onset.	LinkRxCongestionChange	ITP

Description:

```
The notification generated when a link        changes to a new congestion level as specified
by cgspLinkRxCongestionstate object for Received side
congestion
```

Default Message:

$NodeDisplayName ($NodeClliCode) - Link $LinksetName/$SLC: Received side link congestion level is $CongestionState.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgspLinksetSourceDisplayPC	The point code to which this linkset is connected.
cgspLinksetAdjacentDisplayPC	The point code to which this linkset is connected.
cgspLinkDisplayName	A short identifier for each link linkset. This value can be set by system administrator or defaults to the linkset name and SLC formatted as an ASCII string.
cgspLinkRxCongestionState	The Signalling link Received Side congestion status of this link. 0 abate, 1 onset is the received side congestion level
cgspLinksetName	The name of the linkset.
cgspLinkSlc	The Signalling Link Code for this link.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.

Go Top

xmlns:o="urn:schemas-microsoft-com:office:office"
xmlns:w="urn:schemas-microsoft-com:office:word"
xmlns:m="http://schemas.microsoft.com/office/2004/12/omml"
SECTION 8.27

Trap: ciscoGspLinksetRmtHtStateChange

Description:

????????????? The notification generated when the Rate Limit hit level for a linkset changes to a new state. This trap is generated when the rate limit is hit and

style='mso-special-character:line-break'>

????????????? packet actually drop due to rate limit. The value of
class=SpellE>cgspLinksetRmtHtState indicates the new state.

Default Message:

$
class=SpellE>NodeDisplayName ($NodeClliCode) $
class=SpellE>SpDisplayName - The $LinksetNamerate Limit hit level has been changed to $LinksetRateLimitHitLevelState
class=GramE> .

Message Substitution Variables:

href="CommonTrapFields.html">Common Common	Substitution variables common to all traps.
href="NodeTrapFields.html">Node Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgspEventSequenceNumber style='mso-fareast-font-family:"Times New Roman"'>	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgspLinksetDisplayName style='mso-fareast-font-family:"Times New Roman"'>	A short identifier for each linkset. This value can be set by system administrator or defaults to the linkset name.
cgspLinksetSourceDisplayPC style='mso-fareast-font-family:"Times New Roman"'>	The point code to which this linkset is connected.
cgspLinksetAdjacentDisplayPC style='mso-fareast-font-family:"Times New Roman"'>	The point code to which this linkset is connected.
LinksetRmtHtState	Rate Limit hit status of this linkset 0 'no packet drop', 1 'packet drop' for rate limit.
cgspInstNetwork	The network name is used to indicate the network in which this class=SpellE>signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of class=SpellE>signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.
LinksetName	The name of the linkset.

SpDisplayName	Signaling Point Name

xmlns:o="urn:schemas-microsoft-com:office:office"
xmlns:w="urn:schemas-microsoft-com:office:word"
xmlns:m="http://schemas.microsoft.com/office/2004/12/omml"
SECTION 8.28

Trap: ciscoGspLinksetRmtThStateChange

Description:

????????????? The notification generated when the Rate Limit Threshold level for a linkset changes to a???? new state. This trap is generated when the rate ????????????? limit onset threshold is reached. The value of ????????????? cgspLinksetRmtThState indicates the new state.

Default Message:

$NodeDisplayName
($NodeClliCode) $SpDisplayName - The $LinksetName Rate Limit Threshold level is $LinksetRateLimitThresholdState.

Message Substitution Variables:

href="CommonTrapFields.html">Common Common	Substitution variables common to all traps.
href="NodeTrapFields.html">Node Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgspLinksetDisplayName	A short identifier for each linkset. This value can be set by system administrator or defaults to the linkset name.
cgspLinksetSourceDisplayPC	The point code to which this linkset is connected.
cgspLinksetAdjacentDisplayPC	The point code to which this linkset is connected.
LinksetRmtThState	Rate Limit threshold status of this linkset 0 abate, 1 onset.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.
LinksetName	The

	name of the linkset.
SpDisplayName	Signaling Point name

SECTION 8.29

Trap: ciscoItpXuaAsRmtHtStateChange

Description:

?????????????? The notification generated when the Rate Limit hit level for a xua changes to a new state. This trap is generated when the rate limit is hit and ?????????????? packet actually drop due to rate limit. The value of cItpXuaAsRmtHtState indicates the new state.

Default Message:

$NodeDisplayName
($NodeCliCode) $SpDisplayName - The Rate Limit hit level for $ASName has changed to $AsRateLimitHitLevelState.

Message Substitution Variables:

href="CommonTrapFields.html">Common Common	Substitution variables common to all traps.
href="NodeTrapFields.html">Node Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cItpSpCLLICode	Common Language Location Codes (CLLI Codes).
cItpXuaAsDisplayName	This object identifies the AS name associated with the ciscoItpXuaAspStateChange and ciscoItpXuaAsStateChange notifications.
cItpXuaAsRmtHtState	Rate Limit hit status of this xua As, 0 no packet drop, 1 packet drop for Gws rate limit.
ASName	The Application Server name. This name has only local significance.
AsRateLimitHitLevelState	Rate Limit hit status of this xua
spDisplayName	Signaling Point Name

SECTION 8.30

Trap: ciscoItpXuaAsRmtThStateChange

Description:

?????????????? The notification generated when the Rate Limit Threshold level for a xua changes to a new state. This trap is generated when the rate

?????????????? limit onset threshold is reached. The value of
?????????????? cItpXuaAsRmtThState indicates the new state.

Default Message:

$NodeDisplayName
($NodeClliCode) $SpDisplayName - The $ASName Rate Limit threshold level
is $AsRateLimitThresholdState

Message
Substitution Variables:

href="CommonTrapFields.html">Common Common	Substitution variables common to all traps.
href="NodeTrapFields.html">Node Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cItpSpCLLICode	Common Language Location Codes (CLLI Codes).
cItpXuaAsDisplayName	This object identifies the AS name associated with the ciscoItpXuaAspStateChange and ciscoItpXuaAsStateChange notifications.
cItpXuaAsRmtThState	Rate Limit threshold status of xua As 0 abate, 1 onset.
cItpXuaAsName	The Application Server name. This name has only local significance.
ASName	The Application server Name.
AsRateLimitThresholdState	Thershold state values of Application Server
spDisplayName	Signaling Point Name

SECTION 8.31

Trap: ciscoGspLinksetEgressRmtHtStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinksetEgressRmtHtState	Trap	Alarm	Yes	Minor	$NodeDisplayName ($cgspCLLICode) $SpDisplayName- The Egress MSU Rate limit hit level for $cgspLinksetDisplayName has reached the configured limit and packets start dropping.	LinksetEgressRmtHtState	ITP
LinksetEgressRmtHtState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($cgspCLLICode) $SpDisplayName- The Egress MSU Rate limit hit level for $cgspLinksetDisplayName is below the configured limit and packets routing is resumed.	LinksetEgressRmtHtState	ITP

Description:

This notification is generated when the value of cgspLinksetEgressRmtHtState gets changed.

Default Message:

$NodeDisplayName ($cgspCLLICode) $SpDisplayName - The Egress MSU Rate Limit hit level for $cgspLinksetDisplayName has reached the configured limit and packets start dropping.
$NodeDisplayName ($cgspCLLICode) $SpDisplayName - The Egress MSU Rate Limit hit level for $cgspLinksetDisplayName is below the configured limit and packets routing is resumed.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgspLinksetEgressRmtHtState	This objects indicates when the egress rate of MSU reaches limit where packets are blocked as follows: 'true' Indicates that the egress MSU rate reaches the configured limit and packets start dropping. 'false' Indicates that the egress MSU rate is below the configured limit and packets routing is resumed. Represents a boolean value.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgspLinksetDisplayName	A short identifier for each linkset. This value can be set by system administrator or defaults to the linkset name.
cgspLinksetSourceDisplayPC	The point code to which this linkset is connected.
cgspLinksetAdjacentDisplayPC	The point code to which this linkset is connected.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.
cgspLinksetName	The name of the linkset.

Go Top

SECTION 8.32

Trap: ciscoGspLinksetEgressRmtThStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinksetEgressRmtThState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($cgspCLLICode) $SpDisplayName-The Egress MSU Rate limit Threshold level for $cgspLinksetDisplayName has reached or is less than the configured abate-threshold limit.	LinksetEgressRmtThState	ITP
LinksetEgressRmtThState	Trap	Alarm	Yes	Minor	$NodeDisplayName ($cgspCLLICode) $SpDisplayName- The Egress MSU Rate limit Threshold level for $cgspLinksetDisplayName has reached or exceeded the configured onset - Threshold	LinksetEgressRmtThState	ITP

Description:

```
This notification is generated when the value of       cgspLinksetEgressRmtThState gets changed.
```

Default Message:

$NodeDisplayName ($cgspCLLICode)$SpDisplayName - The Egress MSU Rate limit Threshold level for $cgspLinksetDisplayName has reached or exceeded the configured onset-Threshold limit.
$NodeDisplayName ($cgspCLLICode)$SpDisplayName - The Egress MSU Rate limit Threshold level for $cgspLinksetDisplayName has reached or is less than the configured abate-threshold limit.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgspLinksetEgressRmtThState	This objects indicates the state of egress MSU rate as per configured threshold limit as follows: 'true' Indicates that the egress MSU rate reaches or exceeds the configured onset-threshold limit. 'false' Indicates that the egress MSU rate reaches or is less than the configured abate-threshold limit. Represents a boolean value.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgspLinksetDisplayName	A short identifier for each linkset. This value can be set by system administrator or defaults to the linkset name.
cgspLinksetSourceDisplayPC	The point code to which this linkset is connected.
cgspLinksetAdjacentDisplayPC	The point code to which this linkset is connected.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.
cgspLinksetName	The name of the linkset.

Go Top

SECTION 8.33

Trap: ciscoItpXuaAsEgressRmtHtStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AsEgressRmtHtState	Trap	Alarm	Yes	Minor	$NodeDisplayName ($cItpSpCLLICode) $SpDisplayName- The Egress MSU Rate limit hit level for $cItpXuaAsDisplayName has reached the configured limit and packets start dropping.	AsEgressRmtHtState	ITP
AsEgressRmtHtState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($cItpSpCLLICode) $SpDisplayName- The Egress MSU Rate limit hit level for $cItpXuaAsDisplayName is below the configured limit and packets routing is resumed.	AsEgressRmtHtState	ITP

Description:

```
This notification is generated when the        cItpXuaAsEgressRmtHtState object
changes state and is used to indicate loss of packets.
```

Default Message:

$NodeDisplayName ($cItpSpCLLICode) $SpDisplayName - The Egress MSU Rate Limit hit level for $cItpXuaAsDisplayName has reached the configured limit and packets start dropping.
$NodeDisplayName ($cItpSpCLLICode) $SpDisplayName - The Egress MSU Rate Limit hit level for $cItpXuaAsDisplayName is below the configured limit and packets routing is resumed.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cItpXuaAsEgressRmtHtState	This objects indicates when rate of outbound MSU reaches limit where packets are blocked as follows: 'true' Indicates that the egress MSU rate reaches the configured limit and packets start dropping. 'false' Indicates that the egress MSU rate is below the configured limit and packets routing is resumed. Represents a boolean value.
cItpSpCLLICode	Common Language Location Codes (CLLI Codes).
cItpXuaAsDisplayName	This object identifies the AS name associated with the ciscoItpXuaAspStateChange and ciscoItpXuaAsStateChange notifications.
cItpXuaAsName	The Application Server name. This name has only local significance.

Go Top

SECTION 8.34

Trap: ciscoItpXuaAsEgressRmtThStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AsEgressRmtThState	Trap	Alarm	Yes	Minor	$NodeDisplayName ($cItpSpCLLICode) $SpDisplayName - The Egress MSU Rate limit Threshold level for $cItpXuaAsDisplayName has reached or exceeded the configured onset - Threshold	AsEgressRmtThState	ITP
AsEgressRmtThState	Trap	Alarm	Yes	Normal	$NodeDisplayName ($cItpSpCLLICode) $SpDisplayName- The Egress MSU Rate limit Threshold level for $cItpXuaAsDisplayName has reached or is less than the configured abate-threshold limit.	AsEgressRmtThState	ITP

Description:

```
This notification is generated when egress MSU rate reaches the        configured onset-threshold limit and is cleared when egress
MSU rate goes below the configured abate-threshold limit. The
value of cItpXuaAsEgressRmtThState indicates the new state.
```

Default Message:

$NodeDisplayName ($cItpSpCLLICode) $SpDisplayName - The Egress MSU Rate limit Threshold level for $cItpXuaAsDisplayName has reached or exceeded the configured onset-Threshold limit.
$NodeDisplayName ($cItpSpCLLICode) $SpDisplayName - The Egress MSU Rate limit Threshold level for $cItpXuaAsDisplayName has reached or is less than the configured abate-threshold limit.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cItpXuaAsEgressRmtThState	This objects indicates whether outbound MSU to the AS will be rate limited as follows: 'true' Indicates that the egress MSU rate reaches or exceeds the configured onset-threshold limit. 'false' Indicates that the egress MSU rate reaches or is less than the configured abate-threshold limit. Represents a boolean value.
cItpSpCLLICode	Common Language Location Codes (CLLI Codes).
cItpXuaAsDisplayName	This object identifies the AS name associated with the ciscoItpXuaAspStateChange and ciscoItpXuaAsStateChange notifications.
cItpXuaAsName	The Application Server name. This name has only local significance.

Go Top

SECTION 8.35

Trap: ciscoGrtRouteCrdStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GrtRouteCrdStateChange	Trap	Alarm	Yes	Critical	$NodeDisplayName - Circular route is detected corresponding to ($cgspCLLICode) $SpDisplayName and the route $cgrtRouteDisplay on which CRD has hit is marked as prohibited.	GrtRouteCrdStateChange	ITP
GrtRouteCrdStateChange	Trap	Alarm	Yes	Normal	$NodeDisplayName Circular route is detected corresponding to ($cgspCLLICode) $SpDisplayName and the route $cgrtRouteDisplay on which CRD has cleared.	GrtRouteCrdStateChange	ITP

Description:

```
This notification is generated whenever a circular route is       detected on ITP. A Circular route is detected corresponding to
any particular destination point code and the route on which CRD
is detected is marked as probhited.
```

Default Message:

$NodeDisplayName Circular route is detected corresponding to ($cgspCLLICode) $SpDisplayName and the route $cgrtRouteDisplay on which CRD has cleared.
$NodeDisplayName - Circular route is detected corresponding to ($cgspCLLICode) $SpDisplayName and the route $cgrtRouteDisplay on which CRD has hit is marked as prohibited.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgrtRouteCrdTrapState	This objects is used to store value of CRD state of route for particular destination : 'true' Returns True value when CRD hits on ITP. 'false' Returns False value when CRD clears on ITP Represents a boolean value.
cgspEventSequenceNumber	Each event or notification is required to provide a

	sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgrtRouteDisplay	The destination point code associated with the route in display format.
cgrtRouteDestLinksetDisplay	A short identifier for each linkset present inside route table. This value can be set by system administrator or defaults to the linkset name. It will display the linkset name inside the route table.
cgrtRouteDestLinkset	The linkset that the packet is to be forwarded to on matching this route.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.
cgrtRouteMask	The mask used to define which part of cgrtRouteDpc is significant when comparing the cgrtRouteDpc to the destination code point in the packet to be routed.
cgrtRouteDestLsCost	The cost assigned to this linkset matching this route. Higher numbers represent higher cost.
cgrtRouteDpc	The destination point code.

Go Top

SECTION 8.36

Status: SnmpError

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SnmpError	Poll	Alarm	No	Warning	Node $NodeDisplayName has no snmp-able addresses to poll.	SnmpError	ITP
SnmpError	Poll	Alarm	No	Warning	Node $NodeDisplayName is not a supported device or does not have the minimum IOS mib level.	SnmpError	ITP
SnmpError	Poll	Alarm	No	Minor	Node $NodeDisplayName encountered an error during polling: $ErrorString.	SnmpError	ITP
SnmpError	Poll	Alarm	No	Warning	Node $NodeDisplayName has not been configured.	SnmpError	ITP

Description:

The SnmpError status event provides information when MWTM experiences an error during a poll of a Node. The value of SnmpErrorType indicates the type of error. Possible values of SnmpErrorType include:

- NotSnmpable - The Node has no SNMPable interfaces.
- UnsupportedDevice - The Node is not a supported device.
- MibError - An unexpected error occurred.
- NotConfigured - The Node is not configured as an RAN-O device.

Default Message:

- Node $NodeDisplayName has no snmp-able addresses to poll.
- Node $NodeDisplayName is not a supported device or does not have the minimum IOS mib level.
- Node $NodeDisplayName encountered and error during polling: $ErrorString.
- Node $NodeDisplayName has not been configured for a particular MWTM personality.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
SnmpErrorType	Indicates the type of error that occurred.
ErrorString	A detailed error message relative only when ErrorType is MibError.

Operational Information:

- When SnmpErrorType is NotSnmpable check that the Node has not been configured in MWTM to have no SNMPable interfaces. This is most likely a user error.
- When SnmpErrorType is UnsupportedDevice the node is not a supported device or does not have the minimum IOS mib level required by MWTM.
- When SnmpErrorType is MibError an unexpected error has occurred polling a Node. The MessageLog.txt file may have more information related to the error. An ErrorString of 'NoSuchInstance' can occur if MWTM is using a read community string of 'public' for a router but the router has been configured with a non 'public' read community string.
- When SnmpErrorType is NotConfigured the Node is a valid router however it has not been configured for a particular MWTM personality.
- This status could also indicate that device is being accessed via a wrong community string. You can use the MWTM Node SNMP and Credentials Editor to check community strings.

Go Top

SECTION 8.37

Status: ItpMsuRateState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MsuRateState	Poll	Alarm	Yes	Normal	$NodeDisplayName - CPU $msuSlot/$msuBay MSU traffic $msuDirection rate state is acceptable.	MsuRateState	ITP
MsuRateState	Poll	Alarm	Yes	Minor	$NodeDisplayName - CPU $msuSlot/$msuBay MSU traffic $msuDirection rate state is warning.	MsuRateState	ITP
MsuRateState	Poll	Alarm	Yes	Major	$NodeDisplayName - CPU $msuSlot/$msuBay MSU traffic $msuDirection rate state is overloaded.	MsuRateState	ITP

Description:

This status alarm is generated whenthe MsuTrafficRateState transitions between the acceptable , warning and overloaded states.

Default Message:

$NodeDisplayName - CPU $msuSlot/$msuBay MSU traffic $msuDirection rate state is $msuState.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
msuState	MSU Rate State: 'acceptable' - traffic for a specified direction is at the acceptable level. 'warning' - traffic for a specified direction is has reached or exceed warning level but is below the overloaded level. 'overloaded' - traffic for a specified direction has reached or exceeds overloaded level
msuRate	Rate of MSUs over the sample interval mentioned in msuSampleInterval.

msuSize	The average size of MSU over the interval specified by the msuSampleInterval.
msuDirection	The direction of traffic on a processor (transmit or receive).
msuIndex	An index that uniquely represents a processor. This index is assigned arbitrarily by the engine and is not saved over reboots.
msuAcceptableThreshold	This specifies a level of traffic below which the traffic is considered to be acceptable. The value for this object must be less than the values specified by msuWarningThreshold and msuOverloadedThreshold.
msuWarningThreshold	This specifies a level of traffic that indicates a rate that is above acceptable level, but is below level that impacts routing of MSUs. The value for this object must be greater than the values specified by msuAcceptableThreshold and less than msuOverloadedThreshold .
msuOverloadedThreshold	This specifies a level of traffic that indicates a rate that may impact routing of MSUs. The value for this object must be greater than the value specified for msuAcceptableThreshold and msuWarningThreshold.
msuMaxRate	Maximum value for the msuRate
msuNotifyInterval	The length of the interval used to suppress improving state transition notifications.
msuSampleInterval	The length of the interval used to calculate MSU rate.
msuSlot	The slot number of the processor.This will be set to zero when platform does not support processsors in multiple slots.
msuBay	The bay number of the processor.This will be set to zero when platform does not support processsors in multiple bays.

Operational Information:

- If the MSURate is 'acceptable' no action is necessary.
- If the MSURate is 'warning' or 'overloaded' you may want to consider rerouting traffic through other routes.

Go Top

SECTION 8.38

Status: LinkLocalInterfaceStateChange andLinkRemoteInterfaceStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkRemoteInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP remote interface $SctpInterface is Inactive.	LinkRemoteInterfaceStateChange	ITP
LinkRemoteInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP remote interface $SctpInterface is Missing.	LinkRemoteInterfaceStateChange	ITP
LinkRemoteInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP remote interface $SctpInterface is Active.	LinkRemoteInterfaceStateChange	ITP
LinkRemoteInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP remote interface $SctpInterface is Unknown.	LinkRemoteInterfaceStateChange	ITP

Description:

The LinkLocalInterfaceStateChange and LinkRemoteInterfaceStateChangestatus events provide information about a signaling link local and remote SCTP interface. The interface states are:

- Active - The transport address is sending heartbeat messages.
- Inactive - The transport address is not sending heartbeat messages.
- Missing - The configuration of the signaling link refers to a non-existent SCTP interface.
- Unknown - The configured SCTP interface is not used in a current SCTP

association.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP local interface $SctpInterface is $SctpInterfaceState.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP remote interface $SctpInterface is $SctpInterfaceState.

Message Substitution Variables:

Node	Substitution variables for Node related data.
SignalingPoint	Substitution variables for SignalingPoint related data.
Linkset	Substitution variables for Linkset related data.
Link	Substitution variables for Link related data.
SctpInterface	The IP address of the local SCTP interface.
SctpInterfaceState	The current state of the local SCTP interface.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.39

Status: LinkLocalInterfaceStateChange andLinkRemoteInterfaceStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkLocalInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP local interface $SctpInterface is Inactive.	LinkLocalInterfaceStateChange	ITP
LinkLocalInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP local interface $SctpInterface is Missing.	LinkLocalInterfaceStateChange	ITP
LinkLocalInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP local interface $SctpInterface is Active.	LinkLocalInterfaceStateChange	ITP
LinkLocalInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP local interface $SctpInterface is Unknown.	LinkLocalInterfaceStateChange	ITP

Description:

The LinkLocalInterfaceStateChange and LinkRemoteInterfaceStateChangestatus events provide information about a signaling link local and remote SCTP interface. The interface states are:

- Active - The transport address is sending heartbeat messages.
- Inactive - The transport address is not sending heartbeat messages.
- Missing - The configuration of the signaling link refers to a

non-existent SCTP interface.
- Unknown - The configured SCTP interface is not used in a current SCTP
association.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP local interface $SctpInterface is $SctpInterfaceState.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: SCTP remote interface $SctpInterface is $SctpInterfaceState.

Message Substitution Variables:

Node	Substitution variables for Node related data.
SignalingPoint	Substitution variables for SignalingPoint related data.
Linkset	Substitution variables for Linkset related data.
Link	Substitution variables for Link related data.
SctpInterface	The IP address of the local SCTP interface.
SctpInterfaceState	The current state of the local SCTP interface.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.40

Status: ASPALocalInterfaceStateChange andASPARemoteInterfaceStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ASPARemoteInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP remote interface $SctpInterface is Inactive.	ASPARemoteInterfaceStateChange	ITP
ASPARemoteInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP remote interface $SctpInterface is Missing.	ASPARemoteInterfaceStateChange	ITP
ASPARemoteInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP remote interface $SctpInterface is Active.	ASPARemoteInterfaceStateChange	ITP
ASPARemoteInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP remote interface $SctpInterface is Unknown.	ASPARemoteInterfaceStateChange	ITP

Description:

The ASPALocalInterfaceStateChange and ASPARemoteInterfaceStateChangestatus events provide information about an application server process
association local and remote
SCTP interface. The interface states are:

- Active - The transport address is sending heartbeat messages.
- Inactive - The transport address is not sending heartbeat messages.
- Missing - The configuration of the application server process association refers to a non-existent SCTP interface.
- Unknown - The configured SCTP interface is not used in a current SCTP association.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP local interface $SctpInterface is $SctpInterfaceState.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP remote interface $SctpInterface is $SctpInterfaceState.

Message Substitution Variables:

Node	Substitution variables for Node related data.
SignalingPoint	Substitution variables for SignalingPoint related data.
ApplicationServer	Substitution variables for ApplicationServer related data.
ApplicationServerProcessAssociation	Substitution variables for ApplicationServerProcessAssociation related data.
SctpInterface	The IP address of the local SCTP interface.
SctpInterfaceState	The current state of the local SCTP interface.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.41

Status: ASPALocalInterfaceStateChange andASPARemoteInterfaceStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ASPALocalInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP local interface $SctpInterface is Inactive.	ASPALocalInterfaceStateChange	ITP
ASPALocalInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP local interface $SctpInterface is Missing.	ASPALocalInterfaceStateChange	ITP
ASPALocalInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP local interface $SctpInterface is Active.	ASPALocalInterfaceStateChange	ITP
ASPALocalInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP local interface $SctpInterface is Unknown.	ASPALocalInterfaceStateChange	ITP

Description:

The ASPALocalInterfaceStateChange and ASPARemoteInterfaceStateChangestatus events provide information about an application server process association local and remote SCTP interface. The interface states are:

- Active - The transport address is sending heartbeat messages.
- Inactive - The transport address is not sending heartbeat messages.
- Missing - The configuration of the application server process association refers to a non-existent SCTP interface.
- Unknown - The configured SCTP interface is not used in a current SCTP association.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP local interface $SctpInterface is $SctpInterfaceState.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - ASPA $ASName/$ASPAName: SCTP remote interface $SctpInterface is $SctpInterfaceState.

Message Substitution Variables:

Node	Substitution variables for Node related data.
SignalingPoint	Substitution variables for SignalingPoint related data.
ApplicationServer	Substitution variables for ApplicationServer related data.
ApplicationServerProcessAssociation	Substitution variables for ApplicationServerProcessAssociation related data.
SctpInterface	The IP address of the local SCTP interface.
SctpInterfaceState	The current state of the local SCTP interface.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.42

Status: SGMPLocalInterfaceStateChange andSGMPRemoteInterfaceStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SGMPRemoteInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP remote interface $SctpInterface is Inactive.	SGMPRemoteInterfaceStateChange	ITP
SGMPRemoteInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP remote interface $SctpInterface is Missing.	SGMPRemoteInterfaceStateChange	ITP
SGMPRemoteInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP	SGMPRemoteInterfaceStateChange	ITP

					remote interface $SctpInterface is Active.		
SGMPRemoteInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP remote interface $SctpInterface is Unknown.	SGMPRemoteInterfaceStateChange	ITP

Description:

The SGMPLocalInterfaceStateChange and SGMPRemoteInterfaceStateChangestatus events provide information a signalling gateway mated pair local and remote SCTP interface. The interface states are:

- Active - The transport address is sending heartbeat messages.
- Inactive - The transport address is not sending heartbeat messages.
- Missing - The configuration of the SGMP refers to a non-existent SCTP interface.
- Unknown - The configured SCTP interface is not used in a current SCTP association.

Default Message:

- $NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP local interface $SctpInterface is $SctpInterfaceState.
- $NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP remote interface $SctpInterface is $SctpInterfaceState.

Message Substitution Variables:

Node	Substitution variables for Node related data.
SignalingPoint	Substitution variables for SignalingPoint related data.
SgmpAssociation	Substitution variables for SgmpAssociation related data.
SctpInterface	The IP address of the local SCTP interface.
SctpInterfaceState	The current state of the local SCTP interface.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.43

Status: SGMPLocalInterfaceStateChange andSGMPRemoteInterfaceStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SGMPLocalInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP local interface $SctpInterface is Inactive.	SGMPLocalInterfaceStateChange	ITP
SGMPLocalInterfaceStateChange	Poll	Alarm	Yes	Warning	$NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP local interface $SctpInterface is Missing.	SGMPLocalInterfaceStateChange	ITP

SGMPLocalInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP local interface $SctpInterface is Active.	SGMPLocalInterfaceStateChange	ITP
SGMPLocalInterfaceStateChange	Poll	Alarm	Yes	Normal	$NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP local interface $SctpInterface is Unknown.	SGMPLocalInterfaceStateChange	ITP

Description:

The SGMPLocalInterfaceStateChange and SGMPRemoteInterfaceStateChangestatus events provide information a signalling gateway mated pair local and remote SCTP interface. The interface states are:

- Active - The transport address is sending heartbeat messages.
- Inactive - The transport address is not sending heartbeat messages.
- Missing - The configuration of the SGMP refers to a non-existent SCTP interface.
- Unknown - The configured SCTP interface is not used in a current SCTP association.

Default Message:

- $NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP local interface $SctpInterface is $SctpInterfaceState.
- $NodeDisplayName ($NodeClliCode) - SGMP $SGMPName: SCTP remote interface $SctpInterface is $SctpInterfaceState.

Message Substitution Variables:

Node	Substitution variables for Node related data.
SignalingPoint	Substitution variables for SignalingPoint related data.
SgmpAssociation	Substitution variables for SgmpAssociation related data.
SctpInterface	The IP address of the local SCTP interface.
SctpInterfaceState	The current state of the local SCTP interface.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.44

Trap: titanHeartbeat

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CDTHeartbeat	Trap	Event	No	Normal	$NodeDisplayName -- CDT System name: $titanSystemName. Heartbeat recevied.	CDTHeartbeat	ITP

Description:

A titanHeartbeat trap indicates that the serveron the system given by titanSystemName is running and able to send traps. The time the trap was sent is given in titanHeartbeatTimestamp in UTC Time.

Default Message:

Add default message here.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
titanSystemName	An administratively-assigned name for the node that the heartbeat is sent from. By convention, this is the node's fully-qualified domain name.
titanHeartbeatTimestamp	The time, in Universal Time, or UTC, that the heartbeat occurred. Format is YYYY:MM:DD:HH:mm:ss:Z

Go Top

SECTION 8.45

Trap: cItpRouteStateChange and ciscoGrtDestStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ItpRouteStateChange	Trap	Event	No	Warning	$NodeDisplayName ($NodeClliCode) - Had destination state changes suppressed.	ItpRouteStateChange	ITP
ItpRouteStateChange	Trap	Event	No	Informational	$NodeDisplayName ($NodeClliCode) - No destination state changes suppressed.	ItpRouteStateChange	ITP

Description:

These traps provide information when a destination changes states. Large number of destinations prevent generating a single trap per state change. Destination state changes will be sent in bundles and suppressed in certain conditions. Because of the way these traps are designed they can be represented by 1 or more MWTM events. The first event will show whether or not destination state changes were suppressed. The 'NotifInfoSuppressed' key will indicate this state as follows:

- True - Indicates that the device has suppressed the sending of notifications for the remainder of the time interval.
- False- Indicates that the device has not suppressed the sending of notifications in the current time interval.

The second and subsequent events that can be generated will indicate which destinations changed state and what the new 'RouteDestinationState' is as follows:

- Unknown - A destination state of unknown occurs when the destination is a summary route. Unknown state is presented to indicate the protocols do not exchange state information for summary routes in certain configurations.
- Accessible - The destination can be reached by one or more routes specified for the destination. When summary routing is enabled, a destination status will also depend on route table entries that specify less specific matches.
- Inaccessible - Destination can not be reached by any route known to this signaling point.
- Restricted - Traffic has been restricted from being sent to the destination. The restricted state indicates that the primary route for the destination is unavailable or that it is impacted by some network event or failure of resource.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Had destination state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - No destination state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became $RouteDestinationState.

Message Substitution Variables:

CommonNodeSignalingPoint

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
NotifInfoSuppressed	A flag indicating if destination state changes were suppressed, extracted from the trap PDU.
RouteStateChangeCount	The number of destination state changes reflected in this trap, extracted from the trap PDU.
RouteDestinationState	The current state of the destination, extracted from the trap PDU.

RouteTableName	The route table that contains the definition for this destination, extracted from the trap PDU. For the cItpRouteStateChange trap this is the actual route table name and for the ciscoGrtDestStateChange trap this is the ITP network instance name.
RouteDPC	The destination point code specified for the destination, extracted from the trap PDU.
RouteMask	The route mask specified for the RouteDPC, extracted from the trap PDU.
RouteCongestionState	The route congestion state value is valid only for the ciscoGrtDestStateChange trap. One of None, Low, High, or Very High.
SequenceNumber	For the ciscoGrtDestStateChange trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the NotifInfoSuppressed flag indicates that destination changes have been suppressed. It may be necessary to suppress the sending of notifications when a large number destinations change state, due the failure of some common resource. The number of notifications can be controlled by specifying values for NotifWindowTime and NotifMaxPerWindow objects. When the number of destination state changes exceed the specified value the last notification will indicate that notifications are suppressed for the remainder of the window.
- If the RouteState indicates that destinations have become unavailable or restricted you may want to investigate linkset unavailability as the cause.

Diagnostic Commands:

To display the list of routes for a given destination-point-code, use the show cs7 route in EXEC command mode.

show cs7 [*instance-number*] route [*pc* [summary-routes]] [brief | detailed]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
pc	Point code
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a detailed form of the output.

Additional Information:

The following configuration options effect the route and destination status information:

summary-routing-exception

The summary-routing-exception configuration option indicates whether to use the summary route when the fully qualified route is not available. By default the summary-routing-exception option is off and summary route can be used to route MTP3 messages. In a case, when a summary route is available and fully qualified route is unavailable the destination status for the fully qualified route will be restricted rather than unavailable. When summary-routing-exception option is enabled the destination status for the fully qualified route will be unavailable.

max-dynamic-routes

The max-dynamic-routes configuration option defines the maximum number of dynamic routes allowed for the signaling point. If the limit is reached the status of some routes will not reflect the information reflected in the MTP3 management packets.

national-options TFR

This option applies only to ITU and china variants and indicates whether transfer restricted MTP3 management messages will be exchanged between signaling points. When this options is enabled route and destination statuses can display the restricted state.

Note: Changing any of the global configuration options on an operational box will not update all route and destination statuses. Routing behavior will change correctly, although it might not match what would be indicated by some destination statuses. These options are intended to be a one-time configuration before the box is put in service.

Go Top

Trap: cItpRouteStateChange and ciscoGrtDestStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RouteState	Trap	Event	No	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became Accessible.	RouteState	ITP
RouteState	Trap	Event	No	Major	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became Inaccessible.	RouteState	ITP
RouteState	Trap	Event	No	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became Restricted.	RouteState	ITP
RouteState	Trap	Event	No	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became $RouteDestinationState.	RouteState	ITP

Description:

These traps provide information when a destination changes states. Large number of destinations prevent generating a single trap per state change. Destination state changes will be sent in bundles and suppressed in certain conditions. Because of the way these traps are designed they can be represented by 1 or more MWTM events. The first event will show whether or not destination state changes were suppressed. The 'NotifInfoSuppressed' key will indicate this state as follows:

- True - Indicates that the device has suppressed the sending of notifications for the remainder of the time interval.
- False- Indicates that the device has not suppressed the sending of notifications in the current time interval.

The second and subsequent events that can be generated will indicate which destinations changed state and what the new 'RouteDestinationState' is as follows:

- Unknown - A destination state of unknown occurs when the destination is a summary route. Unknown state is presented to indicate the protocols do not exchange state information for summary routes in certain configurations.
- Accessible - The destination can be reached by one or more routes specified for the destination. When summary routing is enabled, a destination status will also depend on route table entries that specify less specific matches.
- Inaccessible - Destination can not be reached by any route known to this signaling point.
- Restricted - Traffic has been restricted from being sent to the destination. The restricted state indicates that the primary route for the destination is unavailable or that it is impacted by some network event or failure of resource.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Had destination state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - No destination state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became $RouteDestinationState.

Message Substitution Variables:

CommonNodeSignalingPoint

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
NotifInfoSuppressed	A flag indicating if destination state changes were suppressed, extracted from the trap PDU.
RouteStateChangeCount	The number of destination state changes reflected in this trap, extracted from the trap PDU.
RouteDestinationState	The current state of the destination, extracted from the trap PDU.
RouteTableName	The route table that contains the definition for this destination, extracted from the trap PDU. For the cItpRouteStateChange trap this is the actual route table name and for the ciscoGrtDestStateChange trap this is the ITP network instance name.
RouteDPC	The destination point code specified for the destination, extracted from the trap PDU.
RouteMask	The route mask specified for the RouteDPC, extracted from the trap PDU.
RouteCongestionState	The route congestion state value is valid only for the ciscoGrtDestStateChange trap. One of None, Low, High, or Very High.
SequenceNumber	For the ciscoGrtDestStateChange trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the NotifInfoSuppressed flag indicates that destination changes have been suppressed. It may be necessary to suppress the sending of notifications when a large number destinations change state, due the failure of some common resource. The number of notifications can be controlled by specifying values for NotifWindowTime and NotifMaxPerWindow objects. When the number of destination state changes exceed the specified value the last notification will indicate that notifications are suppressed for the remainder of the window.
- If the RouteState indicates that destinations have become unavailable or restricted you may want to investigate linkset unavailability as the cause.

Diagnostic Commands:

To display the list of routes for a given destination-point-code, use the show cs7 route in EXEC command mode.

show cs7 [*instance-number*] route [*pc* [summary-routes]] [brief | detailed]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
pc	Point code
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a detailed form of the output.

Additional Information:

The following configuration options effect the route and destination status information:

summary-routing-exception

The summary-routing-exception configuration option indicates whether to use the summary route when the fully qualified route is not available. By default the summary-routing-exception option is off and summary route can be used to route MTP3 messages. In a case, when a summary route is available and fully qualified route is unavailable the destination status for the fully qualified route will be restricted rather than unavailable. When summary-routing-exception option is enabled the destination status for the fully qualified route will be unavailable.

max-dynamic-routes

The max-dynamic-routes configuration option defines the maximum number of dynamic routes allowed for the signaling point. If the limit is reached the status of some routes will not reflect the information reflected in the MTP3 management packets.

national-options TFR

This option applies only to ITU and china variants and indicates whether transfer restricted MTP3 management messages will be exchanged between signaling points. When this options is enabled route and destination statuses can display the restricted state.

Note: Changing any of the global configuration options on an operational box will not update all route and destination statuses. Routing behavior will change correctly, although it might not match what would be indicated by some destination statuses. These options are intended to be a one-time configuration before the box is put in service.

Go Top

SECTION 8.47

Trap: cItpRouteStateChange and ciscoGrtDestStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RouteDestStateInfoSupressed	Trap	Event	No	Warning	$NodeDisplayName ($NodeClliCode) - Had destination state changes suppressed.	RouteDestStateInfoSupressed	ITP
RouteDestStateInfoSupressed	Trap	Event	No	Informational	$NodeDisplayName ($NodeClliCode) - No destination state changes suppressed.	RouteDestStateInfoSupressed	ITP

RouteDestStateInfoSupressed	Trap	Event	No	Warning	$NodeDisplayName ($NodeClliCode) - Had destination state changes suppressed.	RouteDestStateInfoSupressed	ITP
RouteDestStateInfoSupressed	Trap	Event	No	Normal	$NodeDisplayName ($NodeClliCode) - No destination state changes suppressed.	RouteDestStateInfoSupressed	ITP

Description:

These traps provide information when a destination changes states. Large number of destinations prevent generating a single trap per state change. Destination state changes will be sent in bundles and suppressed in certain conditions. Because of the way these traps are designed they can be represented by 1 or more MWTM events. The first event will show whether or not destination state changes were suppressed. The 'NotifInfoSuppressed' key will indicate this state as follows:

- True - Indicates that the device has suppressed the sending of notifications for the remainder of the time interval.
- False- Indicates that the device has not suppressed the sending of notifications in the current time interval.

The second and subsequent events that can be generated will indicate which destinations changed state and what the new 'RouteDestinationState' is as follows:

- Unknown - A destination state of unknown occurs when the destination is a summary route. Unknown state is presented to indicate the protocols do not exchange state information for summary routes in certain configurations.
- Accessible - The destination can be reached by one or more routes specified for the destination. When summary routing is enabled, a destination status will also depend on route table entries that specify less specific matches.
- Inaccessible - Destination can not be reached by any route known to this signaling point.
- Restricted - Traffic has been restricted from being sent to the destination. The restricted state indicates that the primary route for the destination is unavailable or that it is impacted by some network event or failure of resource.

Default Message:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Had destination state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - No destination state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Destination $RouteTableName/$RouteDPC/$RouteMask became $RouteDestinationState.

Message Substitution Variables:

CommonNodeSignalingPoint

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
NotifInfoSuppressed	A flag indicating if destination state changes were suppressed, extracted from the trap PDU.
RouteStateChangeCount	The number of destination state changes reflected in this trap, extracted from the trap PDU.
RouteDestinationState	The current state of the destination, extracted from the trap PDU.
RouteTableName	The route table that contains the definition for this destination, extracted from the trap PDU. For the cItpRouteStateChange trap this is the actual route table name and for the ciscoGrtDestStateChange trap this is the ITP network instance name.
RouteDPC	The destination point code specified for the destination, extracted from the trap PDU.
RouteMask	The route mask specified for the RouteDPC, extracted from the trap PDU.
RouteCongestionState	The route congestion state value is valid only for the ciscoGrtDestStateChange trap. One of None, Low, High, or Very High.
SequenceNumber	For the ciscoGrtDestStateChange trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the NotifInfoSuppressed flag indicates that destination changes have been suppressed. It may be necessary to suppress the sending of notifications when a large number destinations change state, due the failure of some common resource. The number of notifications can be controlled by specifying values for NotifWindowTime and NotifMaxPerWindow objects. When the number of destination state changes exceed the specified value the last notification will indicate that notifications are suppressed for the remainder of the window.
- If the RouteState indicates that destinations have become unavailable or restricted you may want to investigate linkset unavailability as the cause.

Diagnostic Commands:

To display the list of routes for a given destination-point-code, use the show cs7 route in EXEC command mode.

show cs7 [*instance-number*] route [*pc* [summary-routes]] [brief | detailed]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
pc	Point code
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a detailed form of the output.

Additional Information:

The following configuration options effect the route and destination status information:

summary-routing-exception

The summary-routing-exception configuration option indicates whether to use the summary route when the fully qualified route is not available. By default the summary-routing-exception option is off and summary route can be used to route MTP3 messages. In a case, when a summary route is available and fully qualified route is unavailable the destination status for the fully qualified route will be restricted rather than unavailable. When summary-routing-exception option is enabled the destination status for the fully qualified route will be unavailable.

max-dynamic-routes

The max-dynamic-routes configuration option defines the maximum number of dynamic routes allowed for the signaling point. If the limit is reached the status of some routes will not reflect the information reflected in the MTP3 management packets.

national-options TFR

This option applies only to ITU and china variants and indicates whether transfer restricted MTP3 management messages will be exchanged between signaling points. When this options is enabled route and destination statuses can display the restricted state.

Note: Changing any of the global configuration options on an operational box will not update all route and destination statuses. Routing behavior will change correctly, although it might not match what would be indicated by some destination statuses. These options are intended to be a one-time configuration before the box is put in service.

Go Top

SECTION 8.48

Trap: ciscoGrtMgmtStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RouteMgmtStateInfoSuppressed	Trap	Event	No	Warning	$NodeDisplayName ($NodeCliCode) - Had route state changes suppressed.	RouteMgmtStateInfoSuppressed	ITP
RouteMgmtStateInfoSuppressed	Trap	Event	No	Informational	$NodeDisplayName ($NodeCliCode) - No route state changes suppressed.	RouteMgmtStateInfoSuppressed	ITP
RouteMgmtStateInfoSuppressed	Trap	Event	No	Normal	$NodeDisplayName ($NodeCliCode) - No route state changes suppressed.	RouteMgmtStateInfoSuppressed	ITP
RouteMgmtStateInfoSuppressed	Trap	Event	No	Warning	$NodeDisplayName ($NodeCliCode) - Had route state changes suppressed.	RouteMgmtStateInfoSuppressed	ITP

Description:

These traps provide information when a management route changes state. Large number of routes prevent generating a single trap per state change. Management route state changes will be sent in bundles and suppressed in certain conditions. Because of the way these traps are designed they can be represented by 1 or more MWTM events. The first event will

show whether or not management route state changes were suppressed. The 'NotifInfoSuppressed' key will indicate this state as follows:

- True - Indicates that the device has suppressed the sending of notifications for the remainder of the time interval.
- False- Indicates that the device has not suppressed the sending of notifications in the current time interval.

The second and subsequent events that can be generated will indicate which routes changed state and what the new 'RouteState' is as follows:

- Unknown - Status can not be determined.
- Available - Route is available.
- Restricted - Traffic is restricted on route.
- Unavailable - Route is unable to service traffic.
- Deleted - Route has been removed.

Default Message:

- $NodeDisplayName ($NodeClliCode) - Had route state changes suppressed.
- $NodeDisplayName ($NodeClliCode) - No route state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Route $RouteTableName/$RouteDPC/$RouteMask/$RouteDestinationLinkset became $RouteState/$RouteManagementState.

Message Substitution Variables:

CommonNodeSignalingPointLinkset

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
NotifInfoSuppressed	A flag indicating if route state changes were suppressed, extracted from the trap PDU.
RouteStateChangeCount	The number of route state changes reflected in this trap, extracted from the trap PDU.
RouteState	The current state of the route, extracted from the trap PDU.
RouteTableName	The name of the ITP network instance that contains the definition for this route, extracted from the trap PDU.
RouteDPC	The destination point code specified for the route, extracted from the trap PDU.
RouteMask	The route mask specified for the RouteDPC, extracted from the trap PDU.
RouteDestinationLinkset	The linkset that the packet is to be forwarded to on matching this route, extracted from the trap PDU.
RouteDestinationLsCost	The cost assigned to this linkset matching this route, extracted from the trap PDU. Higher numbers represent higher cost.
RouteManagementState	The route management state for this route, extracted from the trap PDU. One of Unknown, Allowed, Restricted, Prohibited, or Deleted.
RouteDynamic	Routes are either static or dynamic. Static routes are created based on configuration information specified by an administrator. Dynamic routes are created as a by product of a network event in certain situations. Dynamic routes are only created when summary routing has been activated. This object indicates whether this route entry is dynamic - True or static - False. Extracted from the trap PDU.
SequenceNumber	SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the NotifInfoSuppressed flag indicates that route changes have been suppressed. It may be necessary to suppress the sending of notifications when a large number routes change state, due the failure of some common resource. The number of notifications can be controlled by specifying values for NotifWindowTime and NotifMaxPerWindow objects. When the number of route state changes exceed the specified value the last notification will indicate that notifications are suppressed for the remainder of the window.
- If the RouteState indicates that routes have become unavailable or restricted you may want to investigate linkset unavailability as the cause.

Diagnostic Commands:

1. To display the list of routes for a given destination-point-code, use the show cs7 route in EXEC command mode.

show cs7 [*instance-number*] route [*pc* [summary-routes]] [brief | detailed]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance

	is instance 0.
pc	Point code
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a comprehensive information with the breakdown of aggregated status into the linkset status and the non-adjacent status.

2. Use "show cs7 linkset" if the detailed route status indicates linkset status as UNAVAIL. If the non-adjacent status is other than AVAIL then investigate the status on the adjacent node.

show cs7 [instance-number] linkset [*ls-name* statistics | state | utilization]

ls-name	(Optional) Linkset name. Displays information for this particular linkset.
statistics	(Optional) Displays link usage statistics.
state	(Optional) Displays MTP3 states for link.
utilization	(Optional) Displays link utilization statistics.

Go Top

SECTION 8.49

Trap: ciscoGrtMgmtStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RouteMgmtState	Trap	Event	No	Normal	$NodeDisplayName ($NodeCliiCode) $SpDisplayName - Route $RouteTableName/$RouteDPC/$RouteMask/$RouteDestinationLinkset became $RouteState/allowed.	RouteMgmtState	ITP
RouteMgmtState	Trap	Event	No	Warning	$NodeDisplayName ($NodeCliiCode) $SpDisplayName - Route $RouteTableName/$RouteDPC/$RouteMask/$RouteDestinationLinkset became $RouteState/restricted.	RouteMgmtState	ITP
RouteMgmtState	Trap	Event	No	Warning	$NodeDisplayName ($NodeCliiCode) $SpDisplayName - Route $RouteTableName/$RouteDPC/$RouteMask/$RouteDestinationLinkset became $RouteState/prohibited.	RouteMgmtState	ITP
RouteMgmtState	Trap	Event	No	Warning	$NodeDisplayName ($NodeCliiCode) $SpDisplayName - Route $RouteTableName/$RouteDPC/$RouteMask/$RouteDestinationLinkset became $RouteState/$RouteManagementState.	RouteMgmtState	ITP
RouteMgmtState	Trap	Event	No	Normal	$NodeDisplayName ($NodeCliiCode) $SpDisplayName - Route $cgrtRouteDisplay_cgspInstNetwork/$cgrtRouteDisplay_cgrtRouteDpc/$cgrtRouteDisplay_cgrtRouteMask/$cgrtRouteDisplay_cgrtRouteDestLinkset became $cgrtRouteStatus/allowed.	RouteMgmtState	ITP
RouteMgmtState	Trap	Event	No	Warning	$NodeDisplayName ($NodeCliiCode) $SpDisplayName - Route $cgrtRouteDisplay_cgspInstNetwork/$cgrtRouteDisplay_cgrtRouteDpc/$cgrtRouteDisplay_cgrtRouteMask/$cgrtRouteDisplay_cgrtRouteDestLinkset became $cgrtRouteStatus/restricted.	RouteMgmtState	ITP
RouteMgmtState	Trap	Event	No	Major	$NodeDisplayName ($NodeCliiCode) $SpDisplayName - Route $cgrtRouteDisplay_cgspInstNetwork/$cgrtRouteDisplay_cgrtRouteDpc/$cgrtRouteDisplay_cgrtRouteMask/$cgrtRouteDisplay_cgrtRouteDestLinkset became $cgrtRouteStatus/prohibited.	RouteMgmtState	ITP
RouteMgmtState	Trap	Event	No	Warning	$NodeDisplayName ($NodeCliiCode) $cgrtRouteDisplay:$cgrtRouteDisplay_cgspInstNetwork - Route $cgrtRouteDisplay_cgspInstNetwork/$cgrtRouteDisplay/$cgrtRouteDisplay_cgrtRouteMask/$cgrtRouteDisplay_cgrtRouteDestLinkset became $cgrtRouteStatus/$cgrtRouteMgmtStatus.	RouteMgmtState	ITP

Description:

These traps provide information when a management route changes state. Large number of routes prevent generating a single trap per state change. Management route state changes will be sent in bundles and suppressed in certain conditions. Because of the way these traps are designed they can be represented by 1 or more MWTM events. The first event will show whether or not management route state changes were suppressed. The 'NotifInfoSuppressed' key will indicate this state as follows:

- True - Indicates that the device has suppressed the sending of notifications for the remainder of the time interval.
- False- Indicates that the device has not suppressed the sending of notifications in the current time interval.

The second and subsequent events that can be generated will indicate which routes changed state and what the new 'RouteState' is as follows:

- Unknown - Status can not be determined.
- Available - Route is available.
- Restricted - Traffic is restricted on route.
- Unavailable - Route is unable to service traffic.
- Deleted - Route has been removed.

Default Message:

- $NodeDisplayName ($NodeClliCode) - Had route state changes suppressed.
- $NodeDisplayName ($NodeClliCode) - No route state changes suppressed.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Route $RouteTableName/$RouteDPC/$RouteMask/$RouteDestinationLinkset became $RouteState/$RouteManagementState.

Message Substitution Variables:

CommonNodeSignalingPointLinkset

Substitution variables common to all traps.	
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
NotifInfoSuppressed	A flag indicating if route state changes were suppressed, extracted from the trap PDU.
RouteStateChangeCount	The number of route state changes reflected in this trap, extracted from the trap PDU.
RouteState	The current state of the route, extracted from the trap PDU.
RouteTableName	The name of the ITP network instance that contains the definition for this route, extracted from the trap PDU.
RouteDPC	The destination point code specified for the route, extracted from the trap PDU.
RouteMask	The route mask specified for the RouteDPC, extracted from the trap PDU.
RouteDestinationLinkset	The linkset that the packet is to be forwarded to on matching this route, extracted from the trap PDU.
RouteDestinationLsCost	The cost assigned to this linkset matching this route, extracted from the trap PDU. Higher numbers represent higher cost.
RouteManagementState	The route management state for this route, extracted from the trap PDU. One of Unknown, Allowed, Restricted, Prohibited, or Deleted.
RouteDynamic	Routes are either static or dynamic. Static routes are created based on configuration information specified by an administrator. Dynamic routes are created as a by product of a network event in certain situations. Dynamic routes are only created when summary routing has been activated. This object indicates whether this route entry is dynamic - True or static - False. Extracted from the trap PDU.
SequenceNumber	SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.

Operational Information:

- If the NotifInfoSuppressed flag indicates that route changes have been suppressed. It may be necessary to suppress the sending of notifications when a large number routes change state, due the failure of some common resource. The number of notifications can be controlled by specifying values for NotifWindowTime and NotifMaxPerWindow objects. When the number of route state changes exceed the specified value the last notification will indicate that notifications are suppressed for the remainder of the window.
- If the RouteState indicates that routes have become unavailable or restricted you may want to investigate linkset unavailability as the cause.

Diagnostic Commands:

1. To display the list of routes for a given destination-point-code, use the show cs7 route in EXEC command mode.

show cs7 [*instance-number*] route [*pc* [summary-routes]] [brief | detailed]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
pc	Point code
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a comprehensive information with the breakdown of aggregated status into the linkset status and the non-adjacent status.

2. Use "show cs7 linkset" if the detailed route status indicates linkset status as UNAVAIL. If the non-adjacent status is other than AVAIL then investigate the status on the adjacent node.

show cs7 [instance-number] linkset [*ls-name* statistics | state | utilization]

ls-name	(Optional) Linkset name. Displays information for this particular linkset.

statistics	(Optional) Displays link usage statistics.
state	(Optional) Displays MTP3 states for link.
utilization	(Optional) Displays link utilization statistics.

Go Top

SECTION 8.50

Trap: ciscoGsccpSOGReceived

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SSOutOfServiceGrant	Trap	Event	No	Informational	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- Gtt Subsystem Out-of-service grant is received.	SSOutOfServiceGrant	ITP

Description:

```
This notification is generated initially when a Subsystem       Out-of-Service Grant is sent in response to a Subsystem
Out-of-Service Request message. The affected PC and affected
SSN are provided with this notification.
```

Default Message:

$NodeDisplayName ($NodeClliCode) $SpDisplayName - Map pointcode/subsystem: $MapPointCode/$MapSubSystem -- Gtt Subsystem Out-of-service grant is received.

Message Substitution Variables:

SignalingPoint

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
Substitution variables for SignalingPoint related data.	
MapPointCode	The point code for GTT MAP entry.
MapSubSystem	The subsystem number (SSN) for GTT MAP entry.
SequenceNumber	For the ciscoGsccpSOGReceived trap only. SequenceNumber is the sequential number of this trap. This number is used to determine if traps have been dropped in the network since the last successful reception of a trap.
cgspEventSequenceNumber	Each event or notification is required to provide a sequence number to be used by the NMS to determine when messages from a particular device are missing. This value will included in each SS7 notification issued by this device.
cgspCLLICode	Common-Language Location Identification Codes (CLLI Codes). This object identifies the physical location of this device and can provide additional informaton on the device type.
cgsccpGttMapDisplayPC	The MAP point code in display format.
cgsccpGttMapDisplaySS	The MAP subsystem number in display format.
cgspInstNetwork	The network name is used to indicate the network in which this signalling point is participating. One or more instances of signalling points can exist in the same physical device. This identifier will be used to correlate instances of signalling points by network. When multiple instance support is not enabled the network name will default to the null string. An octet string specified by an administrator that must be in human-readable form. The names must conform

	to the allowed characters that can be specified via Command Line Interface(CLI). The names cannot contain control character and should not contain leading or trailing white space.
cgsccpGttMapSsn	The subsystem number (SSN) for GTT MAP entry.
cgsccpGttMapPc	The point code for GTT MAP entry.

Go Top

SECTION 8.51

Trap: cSctpExtDestAddressStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SctpExtDestAddressStateChange	Trap	Event	No	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: $DestinationAddress is Active.	SctpExtDestAddressStateChange	ITP
SctpExtDestAddressStateChange	Trap	Event	No	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: $DestinationAddress is Inactive.	SctpExtDestAddressStateChange	ITP
SctpExtDestAddressStateChange	Trap	Event	No	Normal	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Aspa $ASName/$ASPAName: $DestinationAddress is Active.	SctpExtDestAddressStateChange	ITP
SctpExtDestAddressStateChange	Trap	Event	No	Warning	$NodeDisplayName ($NodeClliCode) $SpDisplayName - Aspa $ASName/$ASPAName: $DestinationAddress is Inactive.	SctpExtDestAddressStateChange	ITP
SctpExtDestAddressStateChange	Trap	Event	No	Normal	$NodeDisplayName ($NodeClliCode) - Undeterminable Link or Aspa: $DestinationAddress is Active.	SctpExtDestAddressStateChange	ITP
SctpExtDestAddressStateChange	Trap	Event	No	Warning	$NodeDisplayName ($NodeClliCode) - Undeterminable Link or Aspa: $DestinationAddress is Inactive.	SctpExtDestAddressStateChange	ITP

Description:

The cSctpExtDestAddressStateChange trap provides information when a state changes on a destination address per SCTP association. Each IP/SCTP based link generally has two or more IP addresses. The SS7 link will be active as long as the association can communicate over one IP address. This trap allows NMS to monitor the health of all destination IP addresses. When a this trap is received, MWTM attempts to correlate the trap to a Link or ASP Association. In instances where the SCTP association was terminated and rebuilt MWTM can not make this correlation.
There is a 2 combination key for this trap. The first key is Association type and consists of the following possible values:

- Link - The trap can be correlated to a Link.
- Aspa - The trap can be correlated to an ASP association.
- Unknown - The trap cannot be correlated to a Link or an ASP association.

The second key is DestinationState and indicates the new state represented by this trap.Possible values of DestinationState include:

- Active - Traffic may flow over this link.
- Inactive - Traffic management has detected a failure that prevents activating this link.

Default Messages:

- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Link $LinksetName/$SLC: $DestinationName/$DestinationAddress is $DestinationState.
- $NodeDisplayName ($NodeClliCode) $SpDisplayName - Aspa $ASName/$ASPAName: $DestinationName/$DestinationAddress is $DestinationState.
- $NodeDisplayName ($NodeClliCode) - Undeterminable Link or Aspa: $DestinationName/$DestinationAddress is $DestinationState.

Message Substitution Variables:

CommonNodeSignalingPointLinksetLinkApplicationServerApplicationServerProcessAssociation

Substitution variables common to all traps.
Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the ITP router that sent the trap.
Substitution variables for SignalingPoint related data when the trap has been correlated to a Link or ASP Association.
Substitution variables for Linkset related data when the trap has been correlated to a Link.

Substitution variables for Link related data when the trap has been correlated to a Link.	
Substitution variables for ApplicationServer related data when the trap has been correlated to a ASP Association.	
Substitution variables for ApplicationServerProcessAssociation related data when the trap has been correlated to a ASP Association.	
DestinationAddress	The IP address of the destination from the raw trap PDU.
DestinationName	The IP name associated with the IP address if name resolution is enabled on the MWTM server.
DestinationState	The current state of the destination address from the raw trap PDU.

Operational Information:

- If the state of the destination is 'Active' then no action is necessary.
- If the state of the destination is 'Inactive' this is an indication that the at least one of the secondary methods of communication to a destination point code is unavailable. You may want to investigate using IP based management tools to determine why.

1. For ITP M2PA statistics use "show cs7 m2pa".

show cs7 m2pa {[congestion *ls-name*] | [local-peer port-num] | [peer *ls-name* [*slc*]] | [sctp {parameters | statistics} *ls-name* [*slc*]] | [state *ls-name* [*slc*]] | [statistics *ls-name* [*slc*]]}

congestion	(Optional) Displays M2PA congestion status.
local-peer	(Optional) Displays an M2PA local peer information.
port-num	Port number of the local peer. Valid range is 4096 through 32767.
peer	(Optional) Displays an M2PA remote peer information.
sctp parameters	(Optional) Displays SCTP peer parameters.
sctp statistics	(Optional) Displays SCTP peer statistics.
state	(Optional) Display the M2PA state machine status.
statistics	(Optional) Display the M2PA peer statistics.
timers	(Optional) Displays M2PA timers for RFC.
ls-name	(Optional) Linkset name. Displays information for this particular linkset.
slc	(Optional) Signaling Link Code. Valid range is 0 through 15.

2. For ITP SCTP statistics use "show ip sctp".

show ip sctp {[association [list | parameters *assocId* | statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

3. For ASP information, use the 'show cs7 asp' command in privileged EXEC command.

show cs7 [*instance-number*] asp [m3ua | sua | all | name *asp-name* | asname *as-name*] [statistics [detail] | bindings | detail | event-history]

instance-number	(Optional) Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
m3ua	(Optional) Filter on M3UA.
sua	(Optional) Filter on SUA.
all	Display all ASPs. (Default)
name	(Optional) Filter on ASP name.
asp-name	(Optional) ASP name.
asname	(Optional) Filter on AS name.
statistics	(Optional) Display ASP statistics.
bindings	(Optional) Display ASP bindings

detail	(Optional) Display in detail format.
event-history	(Optional) Display ASP history.

4. For IP routing problems, use the 'show cs7 route' command.

show cs7 [*instance-number*] route [*pc* [summary-routes]] [brief | detailed]

instance-number	Required only if the cs7 multi-instance feature is enabled. Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
pc	Point code
summary-routes	(Optional) Displays summary routes information for the specified pc.
brief	(Optional) Displays a brief form of the output.
detailed	(Optional) Displays a comprehensive information with the breakdown of aggregated status into the linkset status and the non-adjacent status.

5. For connectivity issues use "ip ping" to test connection.
Go Top

SECTION 8.52

Trap: ciscoItpMsuRateState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ItpMsuRateState	Trap	Event	No	Normal	$NodeDisplayName - CPU $cimrMsuProcIndex MSU traffic $cimrMsuTrafficDirection rate state is acceptable.	ItpMsuRateState	ITP
ItpMsuRateState	Trap	Event	No	Minor	$NodeDisplayName - CPU $cimrMsuProcIndex MSU traffic $cimrMsuTrafficDirection rate state is warning.	ItpMsuRateState	ITP
ItpMsuRateState	Trap	Event	No	Major	$NodeDisplayName - CPU $cimrMsuProcIndex MSU traffic $cimrMsuTrafficDirection rate state is overloaded.	ItpMsuRateState	ITP

Description:

This notification is generated once for the interval specified bythe cimrMsuRateNotifyInterval object when the cimrMsuTrafficRateState object has the following state transitions.

'acceptable'
-> 'warning'
'acceptable'
-> 'overloaded'

'warning' -> 'overloaded'

At the end of the interval specified by the cimrMsuRateNotifyInterval object another notification will be generated if the current state is different from state sent in last notification even if the state transition is not one of the above transitions. When the cimrMsuRateNotifyInterval is set to zero all state changes will generate notifications.

Default Message:

$NodeDisplayName - CPU $cimrMsuProcIndex MSU traffic $cimrMsuTrafficDirection rate state is $cimrMsuTrafficRateState.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
	MSU Rate State: 'acceptable' - traffic for a specified direction is at the acceptable level.

cimrMsuTrafficRateState	'warning' - traffic for a specified direction is has reached or exceed warning level but is below the overloaded level. 'overloaded' - traffic for a specified direction has reached or exceeds overloaded level
cimrMsuTrafficRate	Rate of MSUs over the interval specified by the cimrMsuRateSampleInterval object.
cimrMsuTrafficSize	The average size of MSU over the interval specified by the cimrMsuRateSampleInterval object.
cimrMsuTrafficDirection	The direction of traffic on a processor (transmit or receive).
cimrMsuProcIndex	An index that uniquely represents a processor. This index is assigned arbitrarily by the engine and is not saved over reboots.

Operational Information:

- If the MSURate is 'acceptable' no action is necessary.
- If the MSURate is 'warning' or 'overloaded' you may want to consider rerouting traffic through other routes.

Diagnostic Commands:

To display information about the msu rates use command:

show cs7 msu-rates [configuration | current | distribution [msu | percentage]]

configuration	MSU parameters information
current	Current MSU rates
distribution	Number of seconds with certain percentage range or MSU range
msu	Number of seconds with certain MSU range, this is default option
percentage	Number of seconds with certain percentage

Go Top

SECTION 8.53

Trap: ciscoItpXuaAspDestAddrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ciscoItpXuaAspDestAddrStateChange	Trap	Event	No	Major	$NodeDisplayName ($NodeCliiCode) - ASP $cItpXuaAspDisplayName remote IP $cItpXuaAspRemoteIpAddr state is undefined.	ciscoItpXuaAspDestAddrStateChange	ITP
ciscoItpXuaAspDestAddrStateChange	Trap	Event	No	Critical	$NodeDisplayName ($NodeCliiCode) - ASP $cItpXuaAspDisplayName remote IP $cItpXuaAspRemoteIpAddr state is inactive.	ciscoItpXuaAspDestAddrStateChange	ITP
ciscoItpXuaAspDestAddrStateChange	Trap	Event	No	Normal	$NodeDisplayName ($NodeCliiCode) - ASP $cItpXuaAspDisplayName remote IP $cItpXuaAspRemoteIpAddr state is active.	ciscoItpXuaAspDestAddrStateChange	ITP

Description:

```
The notification is generated when a destination
IP address used by ASP changes state.
```

Default Message:

$NodeDisplayName ($NodeCliiCode) - ASP $cItpXuaAspDisplayName

remote IP $cItpXuaAspRemoteIpAddr state is
$cItpXuaAspRemoteIpDestState.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cItpXuaAspRemoteIpDestState	This object contains the remote IP state used to create the association supporting this ASP. The possible remote IP destination states 'undefined' : The state of the remote ip interface is not known or undefined. 'inactive' : The remote ip address of the ASP is not reachable. 'active' : The remote ip address of the ASP is available.
cItpSpCLLICode	Common Language Location Codes (CLLI Codes).
cItpXuaAspDisplayName	This object identifies the ASP name associated with the ciscoItpXuaAspStateChange notification.
cItpXuaAspAssocIdU32	This is the association identifier defined in the Stream Control Transmission Protocol(SCTP) MIB. A value greater than zero indicates a valid association and zero indicates no association.
cItpXuaAspRemoteIpAddr	This object contains the remote IP address used to create the association supporting this ASP.
cItpXuaAspName	The name of the Applicaton Server Process.
cItpXuaAspAddrNum	This object specifies the index for the ASP's remote IP address. The ASP Name in cItpXuaAspName specifies the ASP.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.54

Trap: ciscoItpXuaSgmAssocStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
					$NodeDisplayName ($NodeCliCode) - SGMP		

ciscoItpXuaSgmAssocStateChange	Trap	Event	No	Major	$cItpXuaSgmDisplayName SCTP association state is undefined. Reason: $cItpXuaSgmAssocFailedReason	ciscoItpXuaSgmAssocStateChange	ITP
ciscoItpXuaSgmAssocStateChange	Trap	Event	No	Informational	$NodeDisplayName ($NodeClliCode) - SGMP $cItpXuaSgmDisplayName SCTP association state is closed. Reason: $cItpXuaSgmAssocFailedReason	ciscoItpXuaSgmAssocStateChange	ITP
ciscoItpXuaSgmAssocStateChange	Trap	Event	No	Normal	$NodeDisplayName ($NodeClliCode) - SGMP $cItpXuaSgmDisplayName SCTP association state is established. Reason: $cItpXuaSgmAssocFailedReason	ciscoItpXuaSgmAssocStateChange	ITP
ciscoItpXuaSgmAssocStateChange	Trap	Event	No	Critical	$NodeDisplayName ($NodeClliCode) - SGMP $cItpXuaSgmDisplayName SCTP association state is failed. Reason: $cItpXuaSgmAssocFailedReason	ciscoItpXuaSgmAssocStateChange	ITP
ciscoItpXuaSgmAssocStateChange	Trap	Event	No	Informational	$NodeDisplayName ($NodeClliCode) - SGMP $cItpXuaSgmDisplayName SCTP association state is termPend. Reason: $cItpXuaSgmAssocFailedReason	ciscoItpXuaSgmAssocStateChange	ITP

Description:

```
This notification is generated when the association
used to connect to the SG Mate changes state.
```

Default Message:

$NodeDisplayName ($NodeClliCode) - SGMP $cItpXuaSgmDisplayName
SCTP association state is $cItpXuaSgmAssocState. Reason:
$cItpXuaSgmAssocFailedReason

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

cItpXuaSgmAssocState	`The state of the SG Mate SCTP Association.`
	`The possible XUA ASP SCTP Association States`
	`'undefined'   : The association state is not known or undefined.`
	`'closed'      : The association is closed.`
	`'established' : The association is established with remote end`
	`'failed'      : The association has failed.`
	`'termPend'    : The association has terminated and waiting pending ack.`

cItpSpCLLICode	Common Language Location Codes (CLLI Codes).
cItpXuaSgmDisplayName	This object identifies the SG Mate name associated with the ciscoItpXuaSgmStateChange notification.
cItpXuaSgmAssocId	This is the association identifier defined in the Stream Control Transmission Protocol(SCTP) MIB. A value greater than zero indicates a valid association and zero indicates no association.
cItpXuaSgmAssocFailedReason	The SG Mate SCTP Association failure reason.
cItpXuaSgmName	The name of the SG Mate.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.

list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.55

Trap: ciscoItpXuaSgmDestAddrStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ciscoItpXuaSgmDestAddrStateChange	Trap	Event	No	Major	$NodeDisplayName ($NodeCliCode) - SGMP $cItpXuaSgmDisplayName remote IP $cItpXuaSgmRemoteIpAddr state is undefined .	ciscoItpXuaSgmDestAddrStateChange	ITP
ciscoItpXuaSgmDestAddrStateChange	Trap	Event	No	Critical	$NodeDisplayName ($NodeCliCode) - SGMP $cItpXuaSgmDisplayName remote IP $cItpXuaSgmRemoteIpAddr state is inactive .	ciscoItpXuaSgmDestAddrStateChange	ITP
ciscoItpXuaSgmDestAddrStateChange	Trap	Event	No	Normal	$NodeDisplayName ($NodeCliCode) - SGMP $cItpXuaSgmDisplayName remote IP $cItpXuaSgmRemoteIpAddr state is active .	ciscoItpXuaSgmDestAddrStateChange	ITP

Description:

```
The notification is generated when a destination
IP address used by SG Mate changes state.
```

Default Message:

$NodeDisplayName ($NodeCliCode) - SGMP $cItpXuaSgmDisplayName remote IP $cItpXuaSgmRemoteIpAddr state is $cItpXuaSgmRemoteIpDestState..

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cItpXuaSgmRemoteIpDestState	This object contains the remote IP interface state that is used to create the association supporting this Signalling Gateway Mate. The possible remote IP destination states 'undefined' : The state of the remote ip interface is not known or undefined. 'inactive' : The remote ip address of the ASP is not reachable. 'active' : The remote ip address of the ASP is available.

cItpSpCLLICode	Common Language Location Codes (CLLI Codes).
cItpXuaSgmDisplayName	This object identifies the SG Mate name associated with the ciscoItpXuaSgmStateChange notification.
cItpXuaSgmAssocId	This is the association identifier defined in the Stream Control Transmission Protocol(SCTP) MIB. A value greater than zero indicates a valid association and zero indicates no association.
cItpXuaSgmRemoteIpAddr	This object contains the remote IP address used to create the association supporting this SGM.
cItpXuaSgmName	The name of the SG Mate.
cItpXuaSgmAddrNum	This object specifies the index for the SGM's remote IP address. The SGM Name in cItpXuaSgmName specifies the SGM.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.56

Trap: ciscoItpXuaAspAssocStateChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ciscoItpXuaAspAssocStateChange	Trap	Event	No	Informational	$NodeDisplayName ($NodeCliCode) - ASP $cItpXuaAspDisplayName SCTP association state is closed. Reason: $cItpXuaAspAssocFailedReason	ciscoItpXuaAspAssocStateChange	ITP
ciscoItpXuaAspAssocStateChange	Trap	Event	No	Major	$NodeDisplayName ($NodeCliCode) - ASP $cItpXuaAspDisplayName SCTP association state is undefined. Reason: $cItpXuaAspAssocFailedReason	ciscoItpXuaAspAssocStateChange	ITP
ciscoItpXuaAspAssocStateChange	Trap	Event	No	Normal	$NodeDisplayName ($NodeCliCode) - ASP $cItpXuaAspDisplayName SCTP association state is established. Reason: $cItpXuaAspAssocFailedReason	ciscoItpXuaAspAssocStateChange	ITP
ciscoItpXuaAspAssocStateChange	Trap	Event	No	Critical	$NodeDisplayName ($NodeCliCode) - ASP $cItpXuaAspDisplayName SCTP association state is failed. Reason: $cItpXuaAspAssocFailedReason	ciscoItpXuaAspAssocStateChange	ITP
ciscoItpXuaAspAssocStateChange	Trap	Event	No	Informational	$NodeDisplayName ($NodeCliCode) - ASP $cItpXuaAspDisplayName SCTP association state is termPend. Reason: $cItpXuaAspAssocFailedReason	ciscoItpXuaAspAssocStateChange	ITP

Description:

```
This notification is generated when the association
used to connect to the ASP changes state.
```

Default Message:

$NodeDisplayName ($NodeClliCode) - ASP $cItpXuaAspDisplayName SCTP association state is $cItpXuaAspAssocState. Reason: $cItpXuaAspAssocFailedReason

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cItpXuaAspAssocState	The state of the ASP SCTP Association. The possible XUA ASP SCTP Association States 'undefined' : The association state is not known or undefined. 'closed' : The association is closed. 'established' : The association is established with remote end 'failed' : The association has failed. 'termPend' : The association has terminated and waiting pending ack.
cItpSpCLLICode	Common Language Location Codes (CLLI Codes).
cItpXuaAspDisplayName	This object identifies the ASP name associated with the ciscoItpXuaAspStateChange notification.
cItpXuaAspAssocIdU32	This is the association identifier defined in the Stream Control Transmission Protocol(SCTP) MIB. A value greater than zero indicates a valid association and zero indicates no association.
cItpXuaAspAssocFailedReason	The ASP SCTP Association failure reason.
cItpXuaAspName	The name of the Applicaton Server Process.

Diagnostic Commands:

show ip sctp {[association [list | parameters *assocId* |statistics *assocId*]] | [errors] | [instances] | [statistics]}

association	Specifies an SCTP connection.
list	Current SCTP association.
parameters	SCTP association parameters.
assocId	Association ID number. Valid range is 0 through 1024.
statistics	SCTP association statistics.
errors	SCTP error statistics.
instances	SCTP local peer instances.
statistics	SCTP internal statistics.

Go Top

SECTION 8.57

Status: SignalingPointStateAdded and SignalingPointStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SignalingPointState	Poll	Event	No	Normal	SignalingPoint $NodeDisplayName/$SpDisplayName added in state Active/ActiveReason.	SignalingPointState	ITP
SignalingPointState	Poll	Event	No	Warning	SignalingPoint $NodeDisplayName/$SpDisplayName added in state Warning/WarningReason.	SignalingPointState	ITP

SignalingPointState	Poll	Event	No	Major	SignalingPoint $NodeDisplayName/$SpDisplayName added in state Unknown/UnknownReason.	SignalingPointState	ITP
SignalingPointState	Poll	Event	No	Informational	SignalingPoint $NodeDisplayName/$SpDisplayName added in state Unmanaged/UnmanagedReason.	SignalingPointState	ITP
SignalingPointState	Poll	Event	No	Informational	SignalingPoint $NodeDisplayName/$SpDisplayName added in state $SignalingPointState/$SignalingPointStateReason.	SignalingPointState	ITP
SignalingPointState	Poll	Event	No	Normal	SignalingPoint $NodeDisplayName/$SpDisplayName changed state from $SignalingPointLastState to Active/ActiveReason.	SignalingPointState	ITP
SignalingPointState	Poll	Event	No	Warning	SignalingPoint $NodeDisplayName/$SpDisplayName changed state from $SignalingPointLastState to Warning/WarningReason.	SignalingPointState	ITP
SignalingPointState	Poll	Event	No	Major	SignalingPoint $NodeDisplayName/$SpDisplayName changed state from $SignalingPointLastState to Unknown/UnknownReason.	SignalingPointState	ITP
SignalingPointState	Poll	Event	No	Informational	SignalingPoint $NodeDisplayName/$SpDisplayName changed state from $SignalingPointLastState to Unmanaged/UnmanagedReason.	SignalingPointState	ITP
SignalingPointState	Poll	Event	No	Informational	SignalingPoint $NodeDisplayName/$SpDisplayName changed state from $SignalingPointLastState to $SignalingPointState/$SignalingPointStateReason.	SignalingPointState	ITP

Description:

The SignalingPointStateAdded and SignalingPointStateChanged status events provide information when a SignalingPoint object is added to the MWTM object model or when MWTM detects that the state of a SignalingPoint has changed. The value of SignalingPointState indicates the new state. Possible values of SignalingPointState include:

- Active - The SignalingPoint is fully functional.
- Unknown - An attempt was made to poll a Node for this SignalingPoint but there was an error in polling.
- Warning - The SignalingPoint has been discovered and is capable of traffic flow however some ITP component (Linkset or Link) is not fully functional.
- Unmanaged - The SignalingPoint is not discoverable. It is not on an ITP capable router.
- Deleted - The SignalingPoint has been deleted from the MWTM object database.

Default Message:

- SignalingPoint $NodeDisplayName/$SpDisplayName added in state $SignalingPointState/$SignalingPointStateReason.
- SignalingPoint $NodeDisplayName/$SpDisplayName changed state from $SignalingPointLastState to $SignalingPointState/$SignalingPointStateReason.

Message Substitution Variables:

NodeSignalingPointof the SignalingPoint.

Substitution variables for Node related data.	
Substitution variables for SignalingPoint related data.	
SignalingPointState	The current state of the SignalingPoint.
SignalingPointStateReason	The current state reason of the SignalingPoint.
SignalingPointLastState	The previous state of the SignalingPoint.

Operational Information:

- If the current state of the SignalingPoint is Active no additional action is necessary.
- If the current state of the SignalingPoint is Unknown this is an indication that one of several events has occurred. Check the Node Details for the SignalingPoint in question for the following problems.
  - The SignalingPoint has been unconfigured on the ITP router. MWTM retains knowledge of the SignalingPoint until a user manually deletes it or until is has been in the UNKNOWN state for the UNKNOWN_AGING_TIMEOUT period (default 7 days).
  - A SNMP Timeout has occurred trying to poll the ITP router due to an invalid SNMP community string specification in which case you can reset the community string in the MWTM Node SNMP and Credentials Editor.
  - A SNMP Timeout has occurred because of a network failure in which case you should have your IP administrator check on the network status.
  - A SNMP Timeout has occurred because of a low bandwidth network connection. In this situation you can adjust the SNMP timeout values for Node in the MWTM Node SNMP and Credentials Editor.
  - SNMP is a low priority task on the ITP router and as such if the ITP router is excessively busy with other functions will not reply to the SNMP poll request in a timely manner. In this case the next poll may succeed when the activity on the ITP router clears or you can adjust the SNMP timeout values for Node in the MWTM Node SNMP and Credentials Editor.
  - A SNMP Error has occurred in which case you should contact MWTM support personnel. The MWTM Message log may have more information relating to the problem.
- If the current state of the SignalingPoint is Warning this is an indication that one of the SignalingPoint's Linksets or Links has a state other than active. You should use the Linkset window to determine

the one in error.

- If the current state of the SignalingPoint is Unmanaged this is an indication that MWTM is unable to poll this device due to one of the following reasons.
  - The SignalingPoint is known indirectly by MWTM. In other words, MWTM knows the device exists but there is no known SNMP stack on the device for MWTM to query. This can occur for devices connected to this node via a serial link where there is no known IP address or via a SCTP link where an IP address is known but the first poll for that device fails.
  - During recursive discovery MWTM discovers all seed nodes and attempts to manage them, then flags all SignalingPoints that are adjacent to those seed nodes as Unmanaged
  - A MWTM user has set the SignalingPoint to Unmanaged status, to prevent MWTM from collecting statistics for the SignalingPoint.
- When the current state of the SignalingPoint is Deleted one of the following has occurred.
  - During the MWTM discovery process a SignalingPoint can be recognized by one of it's point codes. At some point during discovery multiple instances of the SignalingPoint are recognized as being the same SignalingPoint and the information from these instances is aggregated to a single instance and the duplicates are deleted.
  - A MWTM user has manually deleted the SignalingPoint.
  - A SignalingPoint that has been in the Unknown state for the period of time specified by the MWTM server property UNKNOWN_AGING_TIMEOUT (default 7 days) will automatically be deleted by MWTM.

Diagnostic Commands:

To display information about the current state of the Links in the Linkset use command:

show cs7 [instance-number] linkset [*ls-name* statistics | state | utilization]

ls-name	(Optional) Linkset name. Displays information for this particular linkset.
statistics	(Optional) Displays link usage statistics.
state	(Optional) Displays MTP3 states for link.
utilization	(Optional) Displays link utilization statistics.

Go Top

SECTION 8.58

Status: ApplicationServerProcessStateAdded and ApplicationServerProcessStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApplicationServerProcessState	Poll	Event	No	Major	ASP $NodeDisplayName/$ASPName changed state from $ASPLastState to Unknown/UnknownReason.	ApplicationServerProcessState	ITP
ApplicationServerProcessState	Poll	Event	No	Informational	ASP $NodeDisplayName/$ASPName added in state $ASPState/$ASPStateReason.	ApplicationServerProcessState	ITP
ApplicationServerProcessState	Poll	Event	No	Informational	ASP $NodeDisplayName/$ASPName changed state from $ASPLastState to $ASPState/$ASPStateReason.	ApplicationServerProcessState	ITP

Description:

The ApplicationServerProcessStateAdded and ApplicationServerProcessStateChanged status events provide information when an ApplicationServerProcess object is added to the MWTM object model or when MWTM detects that the state of an ApplicationServerProcess has changed. The value of ASPState indicates the new state.
Possible values of ASPState include:

- Unknown - The attempt to determine the state of the ASP failed.
- Unmanaged - The state of the ASP cannot be determined as there is not a ITP capable SNMP stack on the Node that hosts this ASP.
- Deleted - The ASP has been deleted from the MWTM object database.

Default Message:

- ASP $NodeDisplayName/$ASPName added in state $ASPState/$ASPStateReason.
- ASP $NodeDisplayName/$ASPName changed state from $ASPLastState to $ASPState/$ASPStateReason.

Message Substitution Variables:

NodeApplicationServerProcessof the ASP.

Substitution variables for Node related data.

Substitution variables for ApplicationServerProcess related data.	
ASPState	The current state of the ApplicationServerProcess.
ASPStateReason	The current state reason of the ASP.
ASPLastState	The previous state of the ApplicationServerProcess.

Operational Information:

- If the current state of the ASP is Unknown, this is an indication that one of several events has occurred:
  - An error occurred polling the Node that this ASP belongs to. The Node and all its ASPs are placed in an unknown state. See the description of the #nodeUnknown Unknown state for a Node for possible causes. for possible causes.
- If the current state of the ASP is Deleted one of the following has occurred.
  - During the MWTM discovery process a Node can be recognized by one of it's point codes or it's IP address. At some point during discovery multiple instances of the Node are recognized as being the same node and the information from these instances is aggregated to a single instance and the duplicates are deleted.
  - A MWTM user has manually deleted the ASP.
  - An ASP that has been in the Unknown state for the period of time specified by the MWTM server property UNKNOWN_AGING_TIMEOUT (default 7 days) will automatically be deleted by MWTM.

Diagnostic Commands:

To display ASP information, use the 'show cs7 asp' command in privileged EXEC command.

show cs7 [*instance-number*] asp [m3ua | sua | all | name *asp-name* | asname *as-name*] [statistics [detail] | bindings | detail | event-history]

instance-number	(Optional) Specifies the instance. The valid range is 0 through 7. The default instance is instance 0.
m3ua	(Optional) Filter on M3UA.
sua	(Optional) Filter on SUA.
all	Display all ASPs. (Default)
name	(Optional) Filter on ASP name.
asp-name	(Optional) ASP name.
asname	(Optional) Filter on AS name.
statistics	(Optional) Display ASP statistics.
bindings	(Optional) Display ASP bindings
detail	(Optional) Display in detail format.
event-history	(Optional) Display ASP history.

Go Top

SECTION 8.59

Status: FolderStateAdded and FolderStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FolderState	Poll	Event	No	Normal	Folder $NodeDisplayName/$FolderDisplayName added in state Active/ActiveReason.	FolderState	ITP
FolderState	Poll	Event	No	Warning	Folder $NodeDisplayName/$FolderDisplayName added in state Warning/WarningReason.	FolderState	ITP
FolderState	Poll	Event	No	Warning	Folder $NodeDisplayName/$FolderDisplayName added in state Unknown/UnknownReason.	FolderState	ITP
FolderState	Poll	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName added in state $FolderState/$FolderStateReason.	FolderState	ITP
FolderState	Poll	Event	No	Normal	Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to Active/ActiveReason.	FolderState	ITP
FolderState	Poll	Event	No	Warning	Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to Warning/WarningReason.	FolderState	ITP
FolderState	Poll	Event	No	Warning	Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to Unknown/UnknownReason.	FolderState	ITP
FolderState	Poll	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to $FolderState/$FolderStateReason.	FolderState	ITP

Description:

The FolderStateAdded and FolderStateChanged status events provide information when a Folder object is added to the MWTM object model or when MWTM detects that the state of a Folder has changed. The value of FolderState indicates the new state.
Possible values of FolderState include:

- Active - The Folder is available and is active. This state implies that all the Interfaces in contained in that folder are in the active state.
- Warning - The Folder is Active however some Interfaces belonging to this Folder is not fully functional.
- Unknown - The attempt to determine the state of the Folder failed.

Default Message:

- Folder $NodeDisplayName/$FolderDisplayName added in state $FolderState/$FolderStateReason.
- Folder $NodeDisplayName/$FolderDisplayName changed state from $FolderLastState to $FolderState/$FolderStateReason.

Message Substitution Variables:

Nodeof the Folder.

Substitution variables for Node related data.	
FolderState	The current state of the Folder.
FolderStateReason	The current state reason of the Folder.
FolderLastState	The previous state of the Folder.

Operational Information:

- If the current state of the Folder is Active no additional action is necessary.
- If the current state of the Folder is Unknown this is an indicator that one of several events has occurred.
  - An error occurred polling the Node that this Folder belongs to. See the description of the #nodeUnknown Unknown state for a Node for possible causes. for possible causes.
- If the current state of the Folder is Warning this is an indication that one of the objects contained in the folder has a state other than active. You could use the Folder details window to determine the object at error.

Go Top

SECTION 8.60

Status: TrapOutOfSequence

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
TrapOutOfSequence	Poll	Event	No	Minor	$NodeDisplayName ($NodeClliCode) - Trap $SequenceNumber received out of sequence. Last trap received was $LastSequenceNumber.	TrapOutOfSequence	ITP

Description:

The TrapOutOfSequence status event provides information when MWTM determines that a trap generated by a router has not reached MWTM. If successive traps received by MWTM for the same router do not contain successive sequence numbers then this event is generated.

Default Message:

- $NodeDisplayName ($NodeClliCode) - Trap $SequenceNumber received out of sequence. Last trap received was $LastSequenceNumber.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
SequenceNumber	The sequence number of the current trap received by MWTM.
LastSequenceNumber	The sequence of the previous trap received by MWTM.

Operational Information:

- The reception of this event could mean that you have networks problems that are preventing the traps from reaching MWTM. SNMP traps use the UDP protocol and as such can be dropped by the network for various reasons.

Go Top

SECTION 8.61

UserAction: SpIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SpIgnoredSet	User Action	Event	No	Informational	SignalingPoint $NodeDisplayName/$SpDisplayName ignore flag is set to $IgnoredFlag by $User.	SpIgnoredSet	ITP

Description:

The SpIgnored UserAction event provides information when a Signaling point's Ignore flag is set by a user. The Ignore flag indicates to SGM whether or not to include the Signaling point in the aggregation algorithm in determining the state of a Node. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The signaling point is to be excluded from state aggregation.
- False - The signaling point is to be included in state aggregation.

Default Message:

SignalingPoint $NodeDisplayName/$SpDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

NodeSignalingPoint	
Substitution variables for Node related data.	
Substitution variables for SignalingPoint related data.	
SpState	The current state of the Signaling point.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the signaling points which are currently ignored select Singaling Points folder in the SGM Main window and sort on the Ignored field.

Go Top

SECTION 8.62

UserAction: LinksetIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinksetIgnoredSet	User Action	Event	No	Informational	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName ignore flag is set to $IgnoredFlag by $User.	LinksetIgnoredSet	ITP

Description:

The LinksetIgnoredSet UserAction event provides information when a Linkset's Ignore flag is set by a user. The Ignore flag indicates to SGM whether or not to include the Linkset in the aggregation algorithm in determining the state of a Node. The value of IgnoredFlag indicates
the new ignore state. Possible values of IgnoredFlag include:

- True - The linkset is to be excluded from state aggregation.
- False - The linkset is to be included in state aggregation.

Default Message:

Linkset $NodeDisplayName/$SpDisplayName/$LinksetName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

NodeSignalingPointLinkset

Substitution variables for Node related data.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
LinksetState	The current state of the Linkset.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated Node states. To find the linksets which are currently ignored select Linkset folder in the SGM Main window and sort on the Ignored field.

Go Top

SECTION 8.63

UserAction: LinkIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkIgnoredSet	User Action	Event	No	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC ignore flag is set to $IgnoredFlag by $User.	LinkIgnoredSet	ITP

Description:

The LinkIgnored UserAction event provides information when a Link's Ignore flag is set by a user. The Ignore flag indicates to SGM whether or not to include the Link in the aggregation algorithm in determining the state of a Node and Linkset. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The link is to be excluded from state aggregation.
- False - The link is to be included in state aggregation.

Default Message:

Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

NodeSignalingPointLinksetLink

Substitution variables for Node related data.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
Substitution variables for Link related data.	
LinkState	The current state of the Link.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated Node and Linkset states. To find the links which are currently ignored select Link folder in the SGM Main window and sort on the Ignored field.

Go Top

SECTION 8.64

UserAction: AsIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AsIgnoredSet	User Action	Event	No	Informational	AS $NodeDisplayName/$SpDisplayName/$ASName ignore flag is set to $IgnoredFlag by $User.	AsIgnoredSet	ITP

Description:

The AsIgnored UserAction event provides information when a Application Server's Ignore flag is set by a user. The Ignore flag indicates to SGM whether or not to include the Application Server in the aggregation algorithm in determining
the state of a Node and Signaling Point. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The Application Server is to be excluded from state aggregation.
- False - The Application Server is to be included in state aggregation.

Default Message:

AS $NodeDisplayName/$SpDisplayName/$ASName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

NodeSignalingPointApplication Server	
Substitution variables for Node related data.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Application Server related data.	
AsState	The current state of the Application Server.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated Node and Signaling Point states. To find the Application Servers which are currently ignored select Application Server folder in the SGM Main window and sort
on the Ignored field.

Go Top

SECTION 8.65

UserAction: AspIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AspIgnoredSet	User Action	Event	No	Informational	ASP $NodeDisplayName/$ASPName ignore flag is set to $IgnoredFlag by $User.	AspIgnoredSet	ITP

Description:

The AspIgnored UserAction event provides information when an Application Server Process's Ignore flag is set
by a user. The Ignore flag indicates to SGM whether or not to include the ASP in the
aggregation algorithm in determining the state of a Node.
The value of IgnoredFlag indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The asp is to be excluded from state aggregation.
- False - The asp is to be included in state aggregation.

Default Message:

ASP $NodeDisplayName/$ASPName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

NodeASP	
Substitution variables for Node related data.	
Substitution variables for ASP related data.	
AspState	The current state of the ASP.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated Node states. To find the asps which are currently ignored select the ASP folder in the SGM Main window and sort on the Ignored field.

Go Top

SECTION 8.66

UserAction: AspaIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AspaIgnoredSet	User Action	Event	No	Informational	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName ignore flag is set to $IgnoredFlag by $User.	AspaIgnoredSet	ITP

Description:

The AspaIgnored UserAction event provides information when an Application Server Process Association's Ignore flag is set by a user. The Ignore flag indicates to SGM whether or not to include the ASPA in the aggregation algorithm in determining the state of a Node, Signaling point and AS.
The value of IgnoredFlag indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The aspa is to be excluded from state aggregation.
- False - The aspa is to be included in state aggregation.

Default Message:

ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

NodeSignalingPointASASPA	
Substitution variables for Node related data.	
Substitution variables for SignalingPoint related data.	
Substitution variables for AS related data.	
Substitution variables for ASPA related data.	
AspaState	The current state of the ASPA.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated Node, Signaling point, and AS states. To find the aspas which are currently ignored select the ASPA folder in the SGM Main window and sort on the Ignored field.

Go Top

SECTION 8.67

UserAction: SgmpIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SgmpIgnoredSet	User Action	Event	No	Informational	SGMP $NodeDisplayName/$SGMPName ignore flag is set to $IgnoredFlag by $User.	SgmpIgnoredSet	ITP

Description:

The SgmpIgnored UserAction event provides information when a Signaling Point Mated Pair's Ignore flag is set by a user. The Ignore flag indicates to SGM whether or not to include the SGMP in the aggregation algorithm in determining the state of a Node and SP. The value of IgnoredFlag indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The sgmp is to be excluded from state aggregation.
- False - The sgmp is to be included in state aggregation.

Default Message:

SGMP $NodeDisplayName/$SGMPName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

NodeSGMP	
Substitution variables for Node related data.	
Substitution variables for SGMP related data.	
SgmpState	The current state of the SGMP.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated Node and Signaling Point states. To find the SGMPs which are currently ignored select the SGMP folder in the SGM Main window and sort on the Ignored field.

Go Top

SECTION 8.68

User Action : FolderIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FolderIgnoredSet	User Action	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName ignore flag is set to $IgnoredFlag by $User.	FolderIgnoredSet	ITP

Go Top

SECTION 8.69

UserAction: SignalingPointUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SignalingPointUserDataUpdated	User Action	Event	No	Informational	SignalingPoint $NodeDisplayName/$SpDisplayName edited by user $User.	SignalingPointUserDataUpdated	ITP

Description:

The SignalingPointUserDataUpdated UserAction event provides information when a SignalingPoint object's user data has been updated by an SGM user.

Default Message:

SP $NodeDisplayName/$SpDisplayName edited by user $User.

Message Substitution Variables:

NodeSignalingPoint	
Substitution variables for Node related data.	
Substitution variables for SignalingPoint related data.	
User	The user who requested the SignalingPoint's data be updated.

Operational Information:

The fields that can be updated for a SignalingPoint include:

- The SignalingPoint's display name used for identifying the SignalingPoint.

- The SignalingPoint's icon used for identifying the SignalingPoint type on the SGM Topology window.
- The SignalingPoint's notes data used for communicating installation dependent information about a SignalingPoint.

Go Top

SECTION 8.70

UserAction: LinksetUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinksetUserDataUpdated	User Action	Event	No	Informational	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName edited by user $User.	LinksetUserDataUpdated	ITP

Description:

The LinksetUserDataUpdated UserAction event provides information when a Linkset object's user data has been updated by an SGM user.

Default Message:

Linkset $NodeDisplayName/$SpDisplayName/$LinksetName edited by user $User.

Message Substitution Variables:

NodeSignalingPointLinkset
Substitution variables for Node related data.
Substitution variables for SignalingPoint related data.
Substitution variables for Linkset related data.
User — The user who requested the Linkset's data be updated.

Operational Information:

The fields that can be updated for a linkset include:

- The linkset's notes data used for communicating installation dependent information about a Linkset.

Go Top

SECTION 8.71

UserAction: LinkUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkUserDataUpdated	User Action	Event	No	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC edited by user $User.	LinkUserDataUpdated	ITP

Description:

The LinkUserDataUpdated UserAction event provides information when a Link object's user data has been updated by an SGM user.

Default Message:

Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC edited by user $User.

Message Substitution Variables:

NodeSignalingPointLinksetLinkset
Substitution variables for Node related data.
Substitution variables for SignalingPoint related data.
Substitution variables for Linkset related data.
Substitution variables for Link related data.
User — The user who requested the Link's data be updated.

Operational Information:

The fields that can be updated for a link include:

- The link's notes data used for communicating installation dependent information about a Link.

Go Top

SECTION 8.72

UserAction: asUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AsUserDataUpdated	User Action	Event	No	Informational	AS $NodeDisplayName/$SpDisplayName/$ASName edited by user $User.	AsUserDataUpdated	ITP

Description:

The asUserDataUpdated UserAction event provides information when an Application Server object's user data has been updated by an SGM user.

Default Message:

AS $NodeDisplayName/$SpDisplayName/$ASName edited by user $User.

Message Substitution Variables:

NodeSignalingPointAS
Substitution variables for Node related data.
Substitution variables for SignalingPoint related data.
Substitution variables for AS related data.
User — The user who requested the AS's data be updated.

Operational Information:

The fields that can be updated for a AS include:

- The AS's notes data used for communicating installation dependent information about an AS.

Go Top

SECTION 8.73

UserAction: aspaUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AspaUserDataUpdated	User Action	Event	No	Informational	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName edited by user $User.	AspaUserDataUpdated	ITP

Description:

The aspaUserDataUpdated UserAction event provides information when an Application Server Process Association object's user data has been updated by an SGM user.

Default Message:

ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName edited by user $User.

Message Substitution Variables:

NodeSignalingPointASASPA
Substitution variables for Node related data.
Substitution variables for SignalingPoint related data.
Substitution variables for AS related data.

Substitution variables for ASPA related data.

User — The user who requested the ASPA's data be updated.

Operational Information:

The fields that can be updated for a ASPA include:

- The ASPA's notes data used for communicating installation dependent information about a ASPA.

Go Top

SECTION 8.74

UserAction: sgmpUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SgmpUserDataUpdated	User Action	Event	No	Informational	SGMP $NodeDisplayName/$SGMPName edited by user $User.	SgmpUserDataUpdated	ITP

Description:

The sgmpUserDataUpdated UserAction event provides information when a Signaling Point Mated Pair object's user data has been updated by an SGM user.

Default Message:

SGMP $NodeDisplayName/$SGMPName edited by user $User.

Message Substitution Variables:

NodeSGMP
Substitution variables for Node related data.
Substitution variables for SGMP related data.

User — The user who requested the SGMP's data be updated.

Operational Information:

The fields that can be updated for a SGMP include:

- The SGMP's notes data used for communicating installation dependent information about a SGMP.

Go Top

SECTION 8.75

UserAction: aspUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AspUserDataUpdated	User Action	Event	No	Informational	Link $NodeDisplayName/$ASPName edited by user $User.	AspUserDataUpdated	ITP

Description:

The aspUserDataUpdated UserAction event provides information when an Application Server Process object's user data has been updated by an SGM user.

Default Message:

ASP $NodeDisplayName/$ASPName edited by user $User.

Message Substitution Variables:

NodeASP
Substitution variables for Node related data.
Substitution variables for ASP related data.

User — The user who requested the ASP's data be updated.

Operational Information:

The fields that can be updated for a ASP include:

- The ASP's notes data used for communicating installation dependent information about a ASP.

Go Top

SECTION 8.76

User Action : FolderUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FolderUserDataUpdated	User Action	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName edited by user $User.	FolderUserDataUpdated	ITP

Go Top

SECTION 8.77

UserAction: SignalingPointDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SignalingPointDeleted	User Action	Event	No	Informational	SignalingPoint $NodeDisplayName/$SpDisplayName deleted by user $User.	SignalingPointDeleted	ITP

Description:

The SignalingPointDeleted UserAction event provides information when a SignalingPoint object's deletion from the SGM object model database is requested.

Default Message:

SignalingPoint $NodeDisplayName/$SpDisplayName deleted by user $User.

Message Substitution Variables:

NodeSignalingPoint
Substitution variables for Node related data.
Substitution variables for SignalingPoint related data.
User — The user who requested the SignalingPoint's data be deleted.

Operational Information:

- The deletion of a SignalingPoint can be requested by the SGM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the SGM server.
- The deletion of a SignalingPoint will also cause all of it's linksets and links to be deleted.

Go Top

SECTION 8.78

UserAction: LinksetDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinksetDeleted	User Action	Event	No	Informational	Linkset $NodeDisplayName/$SpDisplayName/$LinksetName deleted by user $User.	LinksetDeleted	ITP

Description:

The LinksetDeleted UserAction event provides information when a Linkset object's deletion from the SGM object model database is requested.

Default Message:

Linkset $NodeDisplayName/$SpDisplayName/$LinksetName deleted by user $User.

Message Substitution Variables:

NodeSignalingPointLinkset	
Substitution variables for Node related data.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
User	The user who requested the Linkset's data be deleted.

Operational Information:

- The deletion of a linkset will also cause all of it's links to be deleted.
- The indicated User can be the user id associated with the server processes. As a part of normal server discovery operations linksets can be deleted on behalf of the server.

Go Top

SECTION 8.79

UserAction: LinkDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
LinkDeleted	User Action	Event	No	Informational	Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC deleted by user $User.	LinkDeleted	ITP

Description:

The LinkDeleted UserAction event provides information when a Link object's deletion from the SGM object model database is requested.

Default Message:

Link $NodeDisplayName/$SpDisplayName/$LinksetName/$SLC deleted by user $User.

Message Substitution Variables:

NodeSignalingPointLinksetLink	
Substitution variables for Node related data.	
Substitution variables for SignalingPoint related data.	
Substitution variables for Linkset related data.	
Substitution variables for Link related data.	
User	The user who requested the Link's data be deleted.

Operational Information:

The indicated User can be the user id associated with the server processes. As a part of normal server discovery operations links can be deleted on behalf of the server.

Go Top

SECTION 8.80

UserAction: ApplicationServerDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApplicationServerDeleted	User Action	Event	No	Informational	AS $NodeDisplayName/$SpDisplayName/$ASName deleted by user $User.	ApplicationServerDeleted	ITP

Description:

The ApplicationServerDeleted UserAction event provides information when an ApplicationServer object's deletion from the SGM object model database is requested.

Default Message:

AS $NodeDisplayName/$SpDisplayName/$ASName deleted by user $User.

Message Substitution Variables:

NodeSignalingPointApplicationServer	
Substitution variables for Node related data.	
Substitution variables for Node related data.	
Substitution variables for ApplicationServer related data.	
User	The user who requested the Linkset's data be deleted.

Operational Information:

- The deletion of an ApplicationServer will also cause all of it's ApplicationServerProcessAssociations to be deleted.
- The indicated User can be the user id associated with the server processes. As a part of normal server discovery operations ApplicationServer objects can be deleted on behalf of the server.

Go Top

SECTION 8.81

UserAction: ApplicationServerProcessDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApplicationServerProcessDeleted	User Action	Event	No	Informational	ASP $NodeDisplayName/$ASPName deleted by user $User.	ApplicationServerProcessDeleted	ITP

Description:

The ApplicationServerProcessDeleted UserAction event provides information when an ApplicationServerProcess object's deletion from the SGM object model database is requested.

Default Message:

ASP $NodeDisplayName/$ASPName deleted by user $User.

Message Substitution Variables:

NodeApplicationServerProcess	
Substitution variables for Node related data.	
Substitution variables for ApplicationServerProcess related data.	
User	The user who requested the ApplicationServerProcess's data be deleted.

Operational Information:

- The indicated User can be the user id associated with the server processes. As a part of normal server discovery operations ApplicationServerProcess objects can be deleted on behalf of the server.

Go Top

SECTION 8.82

UserAction: SgmpAssociationDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SgmpAssociationDeleted	User Action	Event	No	Informational	SGMP $NodeDisplayName/$SGMPName deleted by user $User.	SgmpAssociationDeleted	ITP

Description:

The SgmpAssociationDeleted UserAction event provides information when an SgmpAssociationDeleted object's deletion from the SGM object model database is requested.

Default Message:

SGMP $NodeDisplayName/$SGMPName deleted by user $User.

Message Substitution Variables:

NodeSgmpAssociation
Substitution variables for Node related data.
Substitution variables for SgmpAssociation related data.
User — The user who requested the SgmpAssociation's data be deleted.

Operational Information:

- The indicated User can be the user id associated with the server processes. As a part of normal server discovery operations SgmpAssociation objects can be deleted on behalf of the server.

Go Top

SECTION 8.83

UserAction: ApplicationServerProcessAssociationDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApplicationServerProcessAssociationDeleted	User Action	Event	No	Informational	ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName deleted by user $User.	ApplicationServerProcessAssociationDeleted	ITP

Description:

The ApplicationServerProcessAssociationDeleted UserAction event provides information when an ApplicationServerProcessAssociation object's deletion from the SGM object model database is requested.

Default Message:

ASPA $NodeDisplayName/$SpDisplayName/$ASName/$ASPAName deleted by user $User.

Message Substitution Variables:

NodeSignalingPointApplicationServerApplicationServerProcessAssociation
Substitution variables for Node related data.
Substitution variables for SignalingPoint related data.
Substitution variables for ApplicationServer related data.
Substitution variables for ApplicationServerProcessAssociation related data.
User — The user who requested the ApplicationServerProcessAssociation's data be deleted.

Operational Information:

- The indicated User can be the user id associated with the server processes. As a part of normal server discovery operations ApplicationServerProcessAssociation objects can be deleted on behalf of the server.

Go Top

SECTION 8.84

User Action : FolderDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
FolderDeleted	User Action	Event	No	Informational	Folder $NodeDisplayName/$FolderDisplayName deleted by user $User.	FolderDeleted	ITP

Go Top

SECTION 9.1

Trap: alarmNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PCRF-Alarm	Trap	Alarm	Yes	Normal	$NodeDisplayName -- $alarmNotifComponentName -- $alarmNotifAlarmDescription. $alarmNotifAdditionalText	PCRF-Alarm	PCRF
PCRF-Alarm	Trap	Alarm	Yes	Indeterminate	$NodeDisplayName -- $alarmNotifComponentName -- $alarmNotifAlarmDescription. $alarmNotifAdditionalText	PCRF-Alarm	PCRF
PCRF-Alarm	Trap	Alarm	Yes	Warning	$NodeDisplayName -- $alarmNotifComponentName -- $alarmNotifAlarmDescription. $alarmNotifAdditionalText	PCRF-Alarm	PCRF
PCRF-Alarm	Trap	Alarm	Yes	Minor	$NodeDisplayName -- $alarmNotifComponentName -- $alarmNotifAlarmDescription. $alarmNotifAdditionalText	PCRF-Alarm	PCRF
PCRF-Alarm	Trap	Alarm	Yes	Major	$NodeDisplayName -- $alarmNotifComponentName -- $alarmNotifAlarmDescription. $alarmNotifAdditionalText	PCRF-Alarm	PCRF
PCRF-Alarm	Trap	Alarm	Yes	Critical	$NodeDisplayName -- $alarmNotifComponentName -- $alarmNotifAlarmDescription. $alarmNotifAdditionalText	PCRF-Alarm	PCRF
PCRF-Alarm	Trap	Alarm	Yes	Normal	$NodeDisplayName -- $alarmNotifComponentName -- $alarmNotifAlarmDescription. $alarmNotifAdditionalText	PCRF-Alarm	PCRF

Description:

```
This is a notification of an alarm generated within the FusionWorks system.
```

Default Message:

$NodeDisplayName -- PCRF component $alarmNotifComponentName. Event type: $alarmNotifEventType. Problem: $alarmNotifSpecificProblem -- Probable Cause: $alarmNotifProbableCause. Description: $alarmNotifAlarmDescription. Additional Text: $alarmNotifAdditionalText.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
alarmNotifComponentName	The name of the component that raised the alarm.
alarmNotifComponentType	The type of the component that raised the alarm.
alarmNotifSpecificProblem	The specific problem of the alarm as defined in the alarm definition.
alarmNotifEventType	The Event Type of the alarm, based on X.733 values.
alarmNotifProbableCause	The Probable Cause of the alarm, based on X.733 values.
alarmNotifPerceivedSeverity	The Perceived Severity of the alarm, based on X.733 values.
alarmNotifNature	The nature of the alarm. Clearable or non-clearable
alarmNotifTimeStamp	The Time Stamp (UTC) representing the time the alarm was generated.
alarmNotifAlarmDescription	A short textual description of the alarm.
alarmNotifAdditionalText	Addition textual information about the particular alarm instance, which is often blank.

Go Top

SECTION 9.2

Trap: applicationStateNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PCRF-ApplicationState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- PCRF application $applicationName -- status is up.	PCRF-ApplicationState	PCRF
PCRF-ApplicationState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- PCRF application $applicationName -- status is impaired.	PCRF-ApplicationState	PCRF
PCRF-ApplicationState	Trap	Alarm	Yes	Major	$NodeDisplayName -- PCRF application $applicationName -- status is down.	PCRF-ApplicationState	PCRF
PCRF-ApplicationState	Trap	Alarm	Yes	Warning	$NodeDisplayName -- PCRF application $applicationName -- status is unknown.	PCRF-ApplicationState	PCRF
PCRF-ApplicationState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- PCRF application $applicationName -- status is up.	PCRF-ApplicationState	PCRF
PCRF-ApplicationState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- PCRF application $applicationName -- status is impaired.	PCRF-ApplicationState	PCRF
PCRF-ApplicationState	Poll	Alarm	Yes	Major	$NodeDisplayName -- PCRF application $applicationName -- status is down.	PCRF-ApplicationState	PCRF
PCRF-ApplicationState	Poll	Alarm	Yes	Warning	$NodeDisplayName -- PCRF application $applicationName -- status is unknown.	PCRF-ApplicationState	PCRF

Description:

```
This notification is issued when an application changes state
```

Default Message:

$NodeDisplayName -- PCRF application $applicationName -- status is up/down/impaired/unknown.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
applicationState	The state of the application. An application entity will be in one of four states - up, down, impaired or unknown
applicationIndex	The index of the application in the table.
applicationName	The name of the application.
applicationLastChange	The time of the last state change for this application.
applicationIndex	The index of the application in the table.

Go Top

SECTION 9.3

Trap: componentStateNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PCRF-ComponentState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- PCRF component $componentName -- status is up.	PCRF-ComponentState	PCRF
PCRF-ComponentState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- PCRF component $componentName -- status is impaired.	PCRF-ComponentState	PCRF
PCRF-ComponentState	Trap	Alarm	Yes	Major	$NodeDisplayName -- PCRF component $componentName -- status is down.	PCRF-ComponentState	PCRF
PCRF-ComponentState	Trap	Alarm	Yes	Warning	$NodeDisplayName -- PCRF component $componentName -- status is unknown.	PCRF-ComponentState	PCRF
PCRF-ComponentState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- PCRF component $componentName -- status is up.	PCRF-ComponentState	PCRF
PCRF-ComponentState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- PCRF component $componentName -- status is impaired.	PCRF-ComponentState	PCRF
PCRF-ComponentState	Poll	Alarm	Yes	Major	$NodeDisplayName -- PCRF component $componentName -- status is down.	PCRF-ComponentState	PCRF
PCRF-ComponentState	Poll	Alarm	Yes	Warning	$NodeDisplayName -- PCRF component $componentName -- status is unknown.	PCRF-ComponentState	PCRF

Description:

```
This notification is issued when a component changes state.
```

Default Message:

$NodeDisplayName -- PCRF component $componentName -- status is up/down/impaired/unknown.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
componentState	This is the current operational state of the component. An application entity will be in one of four states - up, down, impaired or unknown
componentIndex	This contains the index of the component in the table.
componentName	This contains the textual name of the component.
componentLastChange	This is the time of the last state change.
componentIndex	This contains the index of the component in the table.

Go Top

SECTION 9.4

Trap: groupStateNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PCRF-GroupState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- PCRF group $componentInstanceGroupName -- status is up.	PCRF-GroupState	PCRF
PCRF-GroupState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- PCRF group $componentInstanceGroupName -- status is impaired.	PCRF-GroupState	PCRF
PCRF-GroupState	Trap	Alarm	Yes	Major	$NodeDisplayName -- PCRF group $componentInstanceGroupName -- status is down.	PCRF-GroupState	PCRF
PCRF-GroupState	Trap	Alarm	Yes	Warning	$NodeDisplayName -- PCRF group $componentInstanceGroupName -- status is unknown.	PCRF-GroupState	PCRF
PCRF-GroupState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- PCRF group $componentInstanceGroupName -- status is up.	PCRF-GroupState	PCRF
PCRF-GroupState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- PCRF group $componentInstanceGroupName -- status is impaired.	PCRF-GroupState	PCRF
PCRF-GroupState	Poll	Alarm	Yes	Major	$NodeDisplayName -- PCRF group $componentInstanceGroupName -- status is down.	PCRF-GroupState	PCRF
PCRF-GroupState	Poll	Alarm	Yes	Warning	$NodeDisplayName -- PCRF group $componentInstanceGroupName -- status is unknown.	PCRF-GroupState	PCRF

Description:

```
This notification is issued when a component group changes state.
```

Default Message:

$NodeDisplayName -- PCRF group $componentInstanceGroupName -- status is up/down/impaired/unknown.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
componentInstanceGroupState	This is the state of the componentInstanceGroup concerned.An application entity will be in one of four states - up, down, impaired or unknown
componentInstanceGroupIndex	An index for the componentInstanceGroup concerned.
componentInstanceGroupName	The textual name of the componentInstanceGroup concerned.
componentInstanceGroupLastChange	This is the time at which the last state change occured for this componnetInstanceGroup.
componentInstanceGroupIndex	An index for the componentInstanceGroup concerned.

Go Top

SECTION 9.5

Trap: objectStateNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PCRF-ObjectState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- PCRF object $objectInstanceDefinitionName -- status is up.	PCRF-ObjectState	PCRF
PCRF-ObjectState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- PCRF object $objectInstanceDefinitionName -- status is impaired.	PCRF-ObjectState	PCRF
PCRF-ObjectState	Trap	Alarm	Yes	Major	$NodeDisplayName -- PCRF object $objectInstanceDefinitionName -- status is down.	PCRF-ObjectState	PCRF
PCRF-ObjectState	Trap	Alarm	Yes	Warning	$NodeDisplayName -- PCRF object $objectInstanceDefinitionName -- status is unknown.	PCRF-ObjectState	PCRF
PCRF-ObjectState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- PCRF object $objectInstanceDefinitionName -- status is up.	PCRF-ObjectState	PCRF
PCRF-ObjectState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- PCRF object $objectInstanceDefinitionName -- status is impaired.	PCRF-ObjectState	PCRF
PCRF-ObjectState	Poll	Alarm	Yes	Major	$NodeDisplayName -- PCRF object $objectInstanceDefinitionName -- status is down.	PCRF-ObjectState	PCRF
PCRF-ObjectState	Poll	Alarm	Yes	Warning	$NodeDisplayName -- PCRF object $objectInstanceDefinitionName -- status is unknown.	PCRF-ObjectState	PCRF

Description:

```
This notification is issued when an object changes state.
```

Default Message:

$NodeDisplayName -- PCRF object $objectInstanceDefinitionName -- status is up/down/impaired/unknown.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
objectInstanceDefinitionState	This is the operational state of this object. An application entity will be in one of four states - up, down, impaired or unknown
objectInstanceDefinitionIndex	This is the index of the object in the table.
objectInstanceDefinitionLastChange	This is the time of the last state change of this object.
objectInstanceDefinitionName	This is the textual name of the object.
objectInstanceDefinitionIndex	This is the index of the object in the table.

Go Top

SECTION 9.6

Status: PCRFUtilState

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PCRFUtilState	Poll	Alarm	Yes	Normal	$NodeDisplayName - $PcrfStorageType $PcrfStrorageDescr has Normal utilization. Used space $PcrfUsedPercentage %	PCRFUtilState	PCRF
PCRFUtilState	Poll	Alarm	Yes	Warning	$NodeDisplayName - $PcrfStorageType $PcrfStrorageDescr has Warning level utilisation. Used space $PcrfUsedPercentage %	PCRFUtilState	PCRF
PCRFUtilState	Poll	Alarm	Yes	Critical	$NodeDisplayName - $PcrfStorageType $PcrfStrorageDescr has Exceeded the threshold level utilization . Used space $PcrfUsedPercentage %	PCRFUtilState	PCRF

Description:

This event gives storage utilization status on the machine where pcrf or oracle is installed.

Default Message:

$NodeDisplayName - $PcrfStorageType $PcrfStrorageDescr has $PcrfUtilPercentState the threshold level utilization . Used space $PcrfUsedPercentage %. (Critical)
$NodeDisplayName - $PcrfStorageType $PcrfStrorageDescr has $PcrfUtilPercentState level utilisation. Used space $PcrfUsedPercentage %.(Warning)
$NodeDisplayName - $PcrfStorageType $PcrfStrorageDescr has $PcrfUtilPercentState utilization. Used space $PcrfUsedPercentage %.(Normal)

Message Substitution Variables:

Node	Substitution variables for Node related data.
PcrfUtilPercentState	Acceptable(Normal) or Warning(Warning) or Exceeded(Critical)
PcrfStorageType	Storage type
PcrfStrorageDescr	Storage description
PcrfUsedPercentage	Storage space used in percentage

Go Top

SECTION 10.1

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigModified	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was modified.	APN-ConfigModified	PDNGW

Description:

```
A notification of this type is generated when an               entry is generated in the
cgprsAccPtCfgNotifHistTable and
cgprsAccPtCfgNotifEnable is set to true.
```

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	`This object specifies the access point which has been created, changed or modified.`
cgprsAccPtCfgNotifReason	`This object describes the reason of the notification.`

Go Top

SECTION 10.2

Trap: cgprsAccPtSecSrcViolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-UpstreamSecurityViolation	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- Upstream security violation.	APN-UpstreamSecurityViolation	PDNGW

Description:

A notification of this type is generated when security violation as specified by cgprsAccPtVerifyUpStrTpduSrcAddr occurs on an APN.

Default Message:

$NodeDisplayName -- APN ($cgprsAccPtCfgNotifAccPtIndex) Upstream security violation.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtMsAddrType	This object specifies the type of Internet address denoted by cgprsAccPtMsAllocAddr, cgprsAccPtMsNewAddr and cgprsAccPtMsTpduDstAddr.
cgprsAccPtMsAllocAddr	This object specifies the IP address that is assigned to the MS during PDP activation.
cgprsAccPtMsNewAddr	This object specifies the fake IP address that is used by the MS.

Go Top

SECTION 10.3

Trap: cgprsAccPtSecDestViolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-DownstreamSecurityViolation	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- Downstream security violation.	APN-DownstreamSecurityViolation	PDNGW

Description:

A notification of this type is generated when security violation as specified by cgprsAccPtVerifyUpStrTpduDstAddr occurs on an APN.

Default Message:

$NodeDisplayName -- APN ($cgprsAccPtCfgNotifAccPtIndex) Downstream security violation.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtMsAddrType	This object specifies the type of Internet address denoted by cgprsAccPtMsAllocAddr, cgprsAccPtMsNewAddr and cgprsAccPtMsTpduDstAddr.
cgprsAccPtMsAllocAddr	This object specifies the IP address that is assigned to the MS during PDP activation.

cgprsAccPtMsTpduDstAddr	This object specifies the upstream TPDU destination address used by a MS that falls in the reserved range of IP addresses for PLMN devices.

Go Top

SECTION 10.4

Trap: cgprsAccPtMaintenanceNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ServiceMode	Trap	Alarm	Yes	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in maintenance mode.	APN-ServiceMode	PDNGW
APN-ServiceMode	Trap	Alarm	Yes	Normal	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in service.	APN-ServiceMode	PDNGW
APN-ServiceMode	Poll	Alarm	Yes	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in maintenance mode.	APN-ServiceMode	PDNGW
APN-ServiceMode	Poll	Alarm	Yes	Normal	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in service.	APN-ServiceMode	PDNGW

Description:

A notification of this type is generated when APN is placed in maintenance mode which is specified by cgprsAccPtOperationMode.

Default Message:

$NodeDisplayName -- The APN ($cgprsAccPtCfgNotifAccPtIndex) is in maintenance mode.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.

Go Top

SECTION 10.5

Trap: cgprsCgInServiceModeNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	PDNGW
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	PDNGW
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	PDNGW
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	PDNGW
ChargingGatewayMaintenanceMode	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	PDNGW
ChargingGatewayMaintenanceMode	Poll	Alarm	Yes	Warning	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	PDNGW

Description:

A notification of this type is generated when the gateway charging function is in normal mode. This can be identified by cgprsCgServiceMode object.

Default Message:

$NodeDisplayName -- The charging gateway is in service.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 10.6

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is down.	ChargingGatewayState	PDNGW
ChargingGatewayState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is up.	ChargingGatewayState	PDNGW
ChargingGatewayState	Trap	Alarm	Yes	Critical	$NodeDisplayName - The Charging gateway is down	ChargingGatewayState	PDNGW
ChargingGatewayState	Trap	Alarm	Yes	Normal	$NodeDisplayName - The Charging gateway is up	ChargingGatewayState	PDNGW

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	`Type of the GPRS charging gateway or charging related alarm.`
cgprsCgAlarmHistAddrType	`This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.`
cgprsCgAlarmHistAddress	`The IP address that is used to uniquely identify the CG.`
cgprsCgAlarmHistSeverity	`This object indicates the severity of the alarm.`
cgprsCgAlarmHistInfo	`This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.`

Go Top

SECTION 10.7

Trap: cgprsCgGatewaySwitchoverNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewaySwitchover	Trap	Alarm	No	Major	$NodeDisplayName -- The charging gateway switched from $cgprsCgOldChgGatewayAddress to $cgprsCgActiveChgGatewayAddress	ChargingGatewaySwitchover	PDNGW
ChargingGatewaySwitchover	Trap	Alarm	No	Major	$NodeDisplayName -- The charging gateway switched from $cgprsCgGatewayGroupStatusOldCgAddr to $cgprsCgGatewayGroupStatusActiveCgAddr	ChargingGatewaySwitchover	PDNGW

Description:

```
A notification of this type is generated when the        charging gateway is switched, the new charging
gateway is identified by cgprsCgActiveChgGatewayAddress
and the old charging gateway is identified by
cgprsCgOldChgGatewayAddress.
The switchover will happen according to the value set
in cgprsCgGroupSwitchOverTime and the selection of the
new CG will be according to the value set in
cgprsCgSwitchOverPriority.
```

Default Message:

$NodeDisplayName -- The charging gateway switched from $cgprsCgOldChgGatewayAddress to $cgprsCgActiveChgGatewayAddress

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgActiveChgGatewayAddrType	`This object specifies the address type of the active charging gateway.`
cgprsCgActiveChgGatewayAddress	`This object specifies the address of the active charging gateway. The type of address will be represented by cgprsCgActiveChgGatewayAddrType.`
cgprsCgOldChgGatewayAddress	`This object specifies the address of the previous active charging gateway. The type of address will same as the one present in cgprsCgActiveChgGatewayAddrType.`

Go Top

SECTION 10.8

Trap: cGtpPathFailedNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPPathFailed	Trap	Alarm	No	Major	$NodeDisplayName -- Peer ($cGtpLastNoRespToEchoGSNIpAddr) failed to respond to the GTP Echo Request.	GTPPathFailed	PDNGW

Description:

This notification is sent when one of this GSN's peers failed to respond to the GTP 'Echo Request' message for the waiting interval.

Default Message:

$NodeDisplayName -- Peer ($cGtpLastNoRespToEchoGSNIpAddr) failed to respond to the GTP Echo Request.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGtpLastNoRespToEchoGSNIpAddrTyp	This object indicates the type of Internet address by which cGtpLastNoRespToEchoGSNIpAddr is reachable.
cGtpLastNoRespToEchoGSNIpAddr	The IP address of the last peer GSN device that did not reply to an GTP 'Echo Request' message from the local GSN device.

Go Top

SECTION 10.9

Trap: cGgsnSADccaRatingFailed

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCARatingFail	Trap	Alarm	No	Major	$NodeDisplayName -- The Credit Control Server cannot rate a service request for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCARatingFail	PDNGW

Description:

This notification is generated when the credit-control server cannot rate the service request, due to insufficient rating input, incorrect AVP combination or due to an AVP or an AVP value that is not recognized or supported in the rating.

Default Message:

$NodeDisplayName -- The Credit Control Server cannot rate a service request for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 10.10

Trap: cGgsnSADccaEndUsrServDeniedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCAServiceDenied	Trap	Alarm	No	Major	$NodeDisplayName -- The Credit Control Server denied a service request due to service restrictions for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCAServiceDenied	PDNGW

Description:

```
This notification is generated when the credit-          control server denies the service request due to
service restrictions.  On reception of this notif
on category level, the CLCI-C shall discard all future
user traffic for that category on that PDP context and
not attempt to ask for more quotas during the same PDP
context.
```

Default Message:

$NodeDisplayName -- The Credit Control Server denied a service request due to service restrictions for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 10.11

Trap: cGgsnSACsgStateDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CSGState	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The CSG is down.	CSGState	PDNGW
CSGState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The CSG is up.	CSGState	PDNGW

Description:

```
This notification is generated when CSG state goes         down.
```

Default Message:

$NodeDisplayName -- The CSG is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
	This object indicates the type of IP address, for real

cGgsnSANotifCsgRealAddressType	address of the CSG group.
cGgsnSANotifCsgRealAddress	This object indicates the real IP address of the CSG group.
cGgsnSANotifCsgVirtualAddrType	This object indicates the type of IP address, for virtual address of the CSG group.
cGgsnSANotifCsgVirtualAddress	This object indicates the virtual IP address of the CSG group.
cGgsnSANotifCsgPort	This object indicates the port number of the CSG group.

Go Top

SECTION 10.12

Trap: cGgsnSADccaCreditLimReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCACreditLimitReached	Trap	Alarm	No	Major	$NodeDisplayName -- Credit limit reached for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCACreditLimitReached	PDNGW

Description:

This notification is generated when the credit limit is reached. The credit-control server denies the service request since the end user's account could not cover the requested service. Client shall behave exactly as with cGgsnSADccaEndUsrServDeniedNotif.

Default Message:

$NodeDisplayName -- Credit limit reached for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 10.13

Trap: cGgsnSADccaUserUnknownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCAUserUnknown	Trap	Alarm	No	Major	$NodeDisplayName -- User is unknown in the Credit Control Server $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCAUserUnknown	PDNGW

Description:

This notification is generated when the specified end user is unknown in the credit-control server. Such permanent failures cause the client to enter the Idle state. The client shall reject or terminate the PDP context depending on whether the result code was received in a CCA (Initial) or CCA (Update).

Default Message:

$NodeDisplayName -- User is unknown in the Credit Control Server $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 10.14

Trap: cGgsnSADccaAuthRejectedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCAAuthReject	Trap	Alarm	No	Major	$NodeDisplayName -- The Credit Control Server rejected authorization of user $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn.	DCCAAuthReject	PDNGW

Description:

This notification is generated when credit-control server failed in authorization of end user. The PDP context is deleted and category is blacklisted.

Default Message:

$NodeDisplayName -- The Credit Control Server rejected authorization of user $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 10.15

Trap: cGgsnGlobalErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWServiceState	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The gateway service is shutdown. Reason: $cGgsnHistNotifInfo	GWServiceState	PDNGW
GWServiceState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway service is started. Reason: $cGgsnHistNotifInfo	GWServiceState	PDNGW

Description:

```
This notification indicates the occurrence of a gateway        related alarm.
```

Default Message:

$NodeDisplayName -- The gateway service is shutdown.
$NodeDisplayName -- The gateway service is started.
$NodeDisplayName -- MAP-SGSN service is shutdown.
$NodeDisplayName -- MAP-SGSN service is started.
$NodeDisplayName -- No DHCP server is configured.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnGlobalErrorTypes	This object indicates the types of global errors as follows. 'ggsnServiceUp' - Gateway service has started 'ggsnServiceDown' - Gateway service is shutdown 'mapSgsnUp' - MAP-SGSN service has started 'mapSgsnDown' - MAP-SGSN service is shutdown 'noDHCPServer' -- DHCP server is not configured
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

Go Top

SECTION 10.16

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-NoResources	Trap	Alarm	No	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached. Reason: $cGgsnHistNotifInfo	APN-NoResources	PDNGW

Description:

```
This notification indicates the occurrence of a User        related alarm.
```

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 10.17

Trap: cGgsnMaintenanceNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is in maintenance mode.	GWMaintenanceMode	PDNGW
GWMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is in service.	GWMaintenanceMode	PDNGW
GWMaintenanceMode	Poll	Alarm	Yes	Major	$NodeDisplayName -- The gateway is in maintenance mode.	GWMaintenanceMode	PDNGW
GWMaintenanceMode	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is in service.	GWMaintenanceMode	PDNGW

Description:

```
A notification of this type is generated when the gateway is        placed in maintenance mode which is specified by
cGgsnServiceModeStatus.
```

Default Message:

$NodeDisplayName -- The gateway is in maintenance mode.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 10.18

Trap: cGgsnAccessPointNameNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-NoRadius	Trap	Alarm	No	Major	APN $ApnDisplayName on the gateway $NodeDisplayName -- No RADIUS server is configured. $cGgsnHistNotifInfo	APN-NoRadius	PDNGW

Description:

```
This notification indicates the occurrence of a APN        related alarm.
```

Default Message:

$NodeDisplayName -- No RADIUS server is configured. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- IP address allocation failed. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- Access point is not reachable. ($cGgsnNotifAccessPointName)

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
	This object indicates the types access point errors as

cGgsnAccessPointErrorTypes	follows. 'noRadius' - RADIUS Server is not configured. 'ipAllocationFail' - Unable to allocate IP address. 'apnUnreachable' - Unable to reach access point.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 10.19

Trap: cGgsnMemThresholdClearedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWMemoryThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway memory threshold is cleared. The gateway memory overload protection mechanism is disengaged.	GWMemoryThreshold	PDNGW
GWMemoryThreshold	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The gateway memory threshold is reached. The gateway memory overload protection mechanism is engaged.	GWMemoryThreshold	PDNGW

Description:

A notification of this type is generated when the gateway retains the memory and falls below threshold value speficied by cGgsnMemoryThreshold.

Default Message:

$NodeDisplayName -- The gateway memory threshold is cleared. The gateway memory overload protection mechanism is disengaged

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 10.20

Trap: cGgsnAccessPointNameNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-IpAllocationFail	Trap	Alarm	No	Critical	APN $ApnDisplayName on the gateway $NodeDisplayName -- IP address allocation failed. $cGgsnHistNotifInfo	APN-IpAllocationFail	PDNGW

Description:

```
This notification indicates the occurrence of a APN       related alarm.
```

Default Message:

$NodeDisplayName -- No RADIUS server is configured. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- IP address allocation failed. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- Access point is not reachable. ($cGgsnNotifAccessPointName)

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnAccessPointErrorTypes	This object indicates the types access point errors as follows. 'noRadius' - RADIUS Server is not configured. 'ipAllocationFail' - Unable to allocate IP address. 'apnUnreachable' - Unable to reach access point.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 10.21

Trap: cGgsnAccessPointNameNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-Unreachable	Trap	Alarm	No	Critical	APN $ApnDisplayName on the gateway $NodeDisplayName -- Access point is not reachable. $cGgsnHistNotifInfo	APN-Unreachable	PDNGW

Description:

```
This notification indicates the occurrence of a APN       related alarm.
```

Default Message:

$NodeDisplayName -- No RADIUS server is configured. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- IP address allocation failed. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- Access point is not reachable. ($cGgsnNotifAccessPointName)

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnAccessPointErrorTypes	This object indicates the types access point errors as follows. 'noRadius' - RADIUS Server is not configured. 'ipAllocationFail' - Unable to allocate IP address. 'apnUnreachable' - Unable to reach access point.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 10.22

Trap: cGgsnGlobalErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MapSgsnState	Trap	Alarm	Yes	Major	$NodeDisplayName -- MAP-SGSN service is shutdown. Reason: $cGgsnHistNotifInfo	MapSgsnState	PDNGW
MapSgsnState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- MAP-SGSN service is started. Reason: $cGgsnHistNotifInfo	MapSgsnState	PDNGW

Description:

```
This notification indicates the occurrence of a gateway       related alarm.
```

Default Message:

$NodeDisplayName -- The gateway service is shutdown.

$NodeDisplayName -- The gateway service is started.
$NodeDisplayName -- MAP-SGSN service is shutdown.
$NodeDisplayName -- MAP-SGSN service is started.
$NodeDisplayName -- No DHCP server is configured.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnGlobalErrorTypes	This object indicates the types of global errors as follows. 'ggsnServiceUp' - Gateway service has started 'ggsnServiceDown' - Gateway service is shutdown 'mapSgsnUp' - MAP-SGSN service has started 'mapSgsnDown' - MAP-SGSN service is shutdown 'noDHCPServer' -- DHCP server is not configured
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

Go Top

SECTION 10.23

Trap: cGgsnGlobalErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NoDHCPServer	Trap	Alarm	No	Major	$NodeDisplayName -- No DHCP server is configured. Reason: $cGgsnHistNotifInfo	NoDHCPServer	PDNGW

Description:

This notification indicates the occurrence of a gateway related alarm.

Default Message:

$NodeDisplayName -- The gateway service is shutdown.
$NodeDisplayName -- The gateway service is started.
$NodeDisplayName -- MAP-SGSN service is shutdown.
$NodeDisplayName -- MAP-SGSN service is started.
$NodeDisplayName -- No DHCP server is configured.

Message Substitution Variables:

Common	Substitution variables common to all traps.
	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnGlobalErrorTypes	This object indicates the types of global errors as follows. 'ggsnServiceUp' - Gateway service has started 'ggsnServiceDown' - Gateway service is shutdown 'mapSgsnUp' - MAP-SGSN service has started 'mapSgsnDown' - MAP-SGSN service is shutdown 'noDHCPServer' -- DHCP server is not configured
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

Go Top

SECTION 10.24

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-AuthenticationFail	Trap	Alarm	No	Minor	APN $ApnDisplayName on gateway $NodeDisplayName -- A PDP activation failed because of an authentication failure. Reason: $cGgsnHistNotifInfo	APN-AuthenticationFail	PDNGW

Description:

This notification indicates the occurrence of a User related alarm.

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured

	failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 10.25

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-CCRInitFail	Trap	Alarm	No	Minor	APN $ApnDisplayName on gateway $NodeDisplayName -- The TX timer expired before getting a CCR (initial) response. Reason: $cGgsnHistNotifInfo	APN-CCRInitFail	PDNGW

Description:

This notification indicates the occurrence of a User related alarm.

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 10.26

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-QuotaPushFail	Trap	Alarm	No	Minor	APN $ApnDisplayName on gateway $NodeDisplayName -- Quota Push failed to the CSG quota server. Reason: $cGgsnHistNotifInfo	APN-QuotaPushFail	PDNGW

Description:

This notification indicates the occurrence of a User related alarm.

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 10.27

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigCreated	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was created.	APN-ConfigCreated	PDNGW

Description:

A notification of this type is generated when an entry is generated in the cgprsAccPtCfgNotifHistTable and cgprsAccPtCfgNotifEnable is set to true.

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 10.28

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigDeleted	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was deleted.	APN-ConfigDeleted	PDNGW

Description:

A notification of this type is generated when an entry is generated in the cgprsAccPtCfgNotifHistTable and cgprsAccPtCfgNotifEnable is set to true.

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 10.29

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingTransferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.	ChargingTransferState	PDNGW
ChargingTransferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.	ChargingTransferState	PDNGW
ChargingTransferState	Trap	Alarm	Yes	Major	$NodeDisplayName - The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway	ChargingTransferState	PDNGW
ChargingTransferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.	ChargingTransferState	PDNGW

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	`Type of the GPRS charging gateway or charging related alarm.`
cgprsCgAlarmHistAddrType	`This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.`
cgprsCgAlarmHistAddress	`The IP address that is used to uniquely identify the CG.`
cgprsCgAlarmHistSeverity	`This object indicates the severity of the alarm.`
cgprsCgAlarmHistInfo	`This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.`

Go Top

SECTION 10.30

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

ChargingCapacityState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.	ChargingCapacityState	PDNGW
ChargingCapacityState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.	ChargingCapacityState	PDNGW
ChargingCapacityState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.	ChargingCapacityState	PDNGW
ChargingCapacityState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs	ChargingCapacityState	PDNGW

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	`Type of the GPRS charging gateway or charging related alarm.`
cgprsCgAlarmHistAddrType	`This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.`
cgprsCgAlarmHistAddress	`The IP address that is used to uniquely identify the CG.`
cgprsCgAlarmHistSeverity	`This object indicates the severity of the alarm.`
cgprsCgAlarmHistInfo	`This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.`

Go Top

SECTION 10.31

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayEchoState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.	ChargingGatewayEchoState	PDNGW
ChargingGatewayEchoState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway received an echo response from the charging gateway.	ChargingGatewayEchoState	PDNGW
ChargingGatewayEchoState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.	ChargingGatewayEchoState	PDNGW

ChargingGatewayEchoState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway received an echo response from the charging gateway.	ChargingGatewayEchoState	PDNGW

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 10.32

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingCDRBufferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has discarded G-CDRs.	ChargingCDRBufferState	PDNGW
ChargingCDRBufferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.	ChargingCDRBufferState	PDNGW
ChargingCDRBufferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has discarded G-CDRs.	ChargingCDRBufferState	PDNGW
ChargingCDRBufferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.	ChargingCDRBufferState	PDNGW

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
```

```
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 10.33

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging transactions on the gateway are disabled.	ChargingState	PDNGW
ChargingState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging transactions on the gateway are enabled.	ChargingState	PDNGW
ChargingState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging transactions on the gateway are disabled.	ChargingState	PDNGW
ChargingState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging transactions on the gateway are enabled	ChargingState	PDNGW

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.

$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 10.34

Trap: ciscoDiaBaseProtPeerConnectionDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPeerConnectionState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	PDNGW
DiameterPeerConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	PDNGW
DiameterPeerConnectionState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	PDNGW
DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	PDNGW
DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	PDNGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitConnAck.	DiameterPeerConnectionState	PDNGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitICEA.	DiameterPeerConnectionState	PDNGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is elect.	DiameterPeerConnectionState	PDNGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitReturns.	DiameterPeerConnectionState	PDNGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is closing.	DiameterPeerConnectionState	PDNGW

Description:

An ciscoDiaBaseProtPeerConnectionDownNotif notification is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnablePeerConnectionDownNotif is true(1)
2) cdbpPeerStatsState changes to closed(1).
It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.

Default Message:

$NodeDisplayName -- The peer $cdbpPeerId state is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpLocalId	The implementation identification string for the Diameter software in use on the system, for example; 'diameterd'
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 10.35

Trap: ciscoDiaBaseProtPermanentFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPermanentFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol permanent failures for the diameter peer $cdbpPeerId has increased.	DiameterPermanentFailure	PDNGW

Description:

```
An ciscoDiaBaseProtPermanentFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnablePermanentFailureNotif
   is true(1)
2) the value of cdbpPeerStatsPermanentFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol permanent failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsPermanentFailures	This object represents the Number of permanent failures returned to peer.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 10.36

Trap: ciscoDiaBaseProtProtocolErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterProtocolError	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol errors returned to the diameter peer $cdbpPeerId has increased.	DiameterProtocolError	PDNGW

Description:

```
An ciscoDiaBaseProtProtocolErrorNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableProtocolErrorNotif
   is true(1)
2) the value of cdbpPeerStatsProtocolErrors changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol errors returned to the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsProtocolErrors	This object represents the Number of protocol errors returned to peer, but not including redirects.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 10.37

Trap: ciscoDiaBaseProtTransientFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterTransientFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol transient failures for the diameter peer $cdbpPeerId has increased.	DiameterTransientFailure	PDNGW

Description:

```
An ciscoDiaBaseProtTransientFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableTransientFailureNotif
   is true(1)
2) the value of cdbpPeerStatsTransientFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol transient failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsTransientFailures	This object represents the transient failure count.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 10.38

Trap: cegCongestionClearedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-GW-CongestionState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus.	EPC-GW-CongestionState	PDNGW
EPC-GW-CongestionState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus. This gateway is rejecting all new calls.	EPC-GW-CongestionState	PDNGW
EPC-GW-CongestionState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus. This gateway is rejecting low priority calls.	EPC-GW-CongestionState	PDNGW
EPC-GW-CongestionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The EPC Gateway congestion status is normal.	EPC-GW-CongestionState	PDNGW
EPC-GW-CongestionState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The EPC Gateway congestion status is high. This gateway is rejecting all new calls.	EPC-GW-CongestionState	PDNGW
EPC-GW-CongestionState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- The EPC Gateway congestion status is low. This gateway is rejecting low priority calls.	EPC-GW-CongestionState	PDNGW

Description:

```
The gateway sends this notification, when       the gateway congestion level goes below
cegLowCongestionThreshold value.
This gives an indication that the gateway
has recovered from congestion and it can
accept all calls.
```

Default Message:

$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegVersion	This object represents the current version of the PGW or SGW software running on the gateway. Display format: : :.
cegCongestionStatus	This object represents the gateway congestion status. INTEGER is unknown
cegCongestionDfpWeight	This object represents the dfp value, which is used to measure the congestion level in the gateway.
cegCongestionLowThreshold	This object represents the low threshold for congestion. Congestion DFP metric considers the current CPU memory usage and number of bearers open. On reaching the low congestion threshold, based on the ARP, high priority calls are accepted and those with a lower priority are rejected. When the gateway congestion level goes below this value, the gateway send cegCongestionClearedNotif notification. This notification would indicate that the gateway has recovered from congestion.

Go Top

SECTION 10.39

Trap: cegqCacMaxPdpExceededNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-MaxPdpExceeded	Trap	Alarm	No	Major	$NodeDisplayName -- The number of pdps on the gateway has reached the user-configured maximum of $cegqCacMaxPdpContext for the CAC policy $cegqCacMaxPdpContext_cegqCacPolicyName.	EPC-QOS-MaxPdpExceeded	PDNGW

Description:

```
This notification is sent when the number of pdps on the       gateway has reached the user-configured maximum (or threshold).
```

Default Message:

$NodeDisplayName -- The number of pdps on the gateway has reached the user-configured maximum of $cegqCacMaxPdpContext for the CAC policy $cegqCacMaxPdpContext_cegqCacPolicyName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqCacMaxPdpContext	This object defines maximum number that can be created. If total number of activated pdp exceeds the maximum number, the pdp request will be rejected. Value '0' means there is no limit on pdp creation.
cegqCacPolicyName	This object is the CAC policy name which will be attached to one or more APN's.

Go Top

SECTION 10.40

Trap: cegqCacUpgBRateBearerRejNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-BearerRejected	Trap	Alarm	No	Major	$NodeDisplayName -- The gateway is rejecting bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate	EPC-QOS-BearerRejected	PDNGW

Description:

```
This notification is sent when bearers are Rejected/Downgraded       by CAC due to requesting for higher bit rate than
user-configured maximum for a certain QCI class.
```

Default Message:

$NodeDisplayName -- The gateway is rejecting bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqCacQciReject	This object is to specify whether the requested MBR/GBR be downgraded or bearer to be rejected if the requested MBR/GBR exceeds the value set in cegqCacQciBitRateType. 'true' - The request will be rejected if exceeded. 'false' - The requested MBR will be downgraded if exceeded. Represents a boolean value.
cegqCacQciBitRate	This object specifies the MBR/GBR allowed for the QCI defined by cegqCacQci.
cegqCacQci	This object specifies the QCI for which MBR/GBR in uplink/downlink has to be set. When the ratetype is set to guaranteed,QCI1-QCI4 are allowed. When the ratetype is set to maximum,QCI1-QCI9 are allowed.
cegqCacQciBitRateType	This object specifies the type of bit rate applicable for QCI denoted by cegqCacQci.
cegqCacQciDirection	This object specifies the direction of traffic.
cegqCacPolicyName	This object is the CAC policy name which will be attached to one or more APN's.

Go Top

SECTION 10.41

Trap: cegqCacUpgBRateBearerRejNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-BearerDowngraded	Trap	Alarm	No	Minor	$NodeDisplayName -- The gateway is downgrading bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate	EPC-QOS-BearerDowngraded	PDNGW

Description:

```
This notification is sent when bearers are Rejected/Downgraded       by CAC due to requesting for higher bit rate than
user-configured maximum for a certain QCI class.
```

Default Message:

$NodeDisplayName -- The gateway is rejecting bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqCacQciReject	This object is to specify whether the requested MBR/GBR be downgraded or bearer to be rejected if the requested MBR/GBR exceeds the value set in cegqCacQciBitRateType. 'true' - The request will be rejected if exceeded. 'false' - The requested MBR will be downgraded if exceeded. Represents a boolean value.
cegqCacQciBitRate	This object specifies the MBR/GBR allowed for the QCI defined by cegqCacQci.
cegqCacQci	This object specifies the QCI for which

	MBR/GBR in uplink/downlink has to be set. When the ratetype is set to guaranteed,QCI1-QCI4 are allowed. When the ratetype is set to maximum,QCI1-QCI9 are allowed.
cegqCacQciBitRateType	This object specifies the type of bit rate applicable for QCI denoted by cegqCacQci.
cegqCacQciDirection	This object specifies the direction of traffic.
cegqCacPolicyName	This object is the CAC policy name which will be attached to one or more APN's.

Go Top

SECTION 10.42

Trap: cegqQciBWMaxReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-MaxBandwidthReached	Trap	Alarm	No	Warning	$NodeDisplayName -- The bandwidth available is fully utilized. No more bearers can be admitted for this QCI class.	EPC-QOS-MaxBandwidthReached	PDNGW

Description:

```
This notification is sent when the bandwidth allocated for a        certain QCI class has been fully utilized and no further bearer
can be admitted for this QCI class. The notification is sent
when the bandwidth pool utilization reaches the value in
the object cegqBWPoolQciAbsVal.
```

Default Message:

$NodeDisplayName -- The bandwidth available is fully utilized. No more bearers can be admitted for this QCI class.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqBWPoolQciAbsVal	This object denotes the absolute value of bandwidth allocated for the QCI set in cegqBWPoolQci.
cegqBWPoolQciAvailBw	This object denotes the absolute available bandwidth left unused for QCI set in cegqBWPoolQci.
cegqBWPoolQci	This object defines the QCI for which the allocation of bandwidth is needed.
cegqCacBWPoolName	This object is the name of the virtual bandwidth pool which will be attached to the APN.

Go Top

SECTION 10.43

Trap: cIscsiInstSessionFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-InstanceSessionState	Trap	Alarm	No	Warning	$NodeDisplayName - The active session has failed for the remote node - $cIscsiInstLastSsnRmtNodeName.	iSCSI-InstanceSessionState	PDNGW

Description:

```
Sent when an active session is failed by either the initiator        or the target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The active session has failed for the remote node $cIscsiInstLastSsnRmtNodeName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiInstSsnFailures	This object counts the number of times a session belonging to this instance has been failed.
cIscsiInstLastSsnFailureType	The counter object in the cIscsiInstSsnErrorStatsTable that was incremented when the last session failure occurred. If the reason for failure is not found in the cIscsiInstSsnErrorStatsTable, the value { 0.0 } is used instead.
cIscsiInstLastSsnRmtNodeName	An octet string describing the name of the remote node from the failed session.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.

Go Top

SECTION 10.44

Trap: cIscsiIntrLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-InitiatorLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.	iSCSI-InitiatorLoginStatus	PDNGW

Description:

```
Sent when a login is failed by a initiator.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiIntrLastTgtFailureAddrType	The type of Internet Network Address in cIscsiIntrLastTgtFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address

	which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiIntrLoginFailures	This object counts the number of times a login attempt from this local initiator has failed.
cIscsiIntrLastFailureType	The type of the most recent failure of a login attempt from this initiator, represented as the OID of the counter object in cIscsiInitiatorLoginStatsTable for which the relevant instance was incremented. A value of 0.0 indicates a type which is not represented by any of the counters in cIscsiInitiatorLoginStatsTable.
cIscsiIntrLastTgtFailureName	An octet string giving the name of the target that failed the last login attempt.
cIscsiIntrLastTgtFailureAddr	An Internet Network Address giving the host address of the target that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

SECTION 10.45

Trap: cIscsiTgtLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-TargetLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.	iSCSI-TargetLoginStatus	PDNGW

Description:

```
Sent when a login is failed by a target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiTgtLastIntrFailureAddrType	The type of Internet Network Address in cIscsiTgtLastIntrFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiTgtLoginFailures	This object counts the number of times a login attempt to this local target has failed.
cIscsiTgtLastFailureType	The type of the most recent failure of a login attempt to this target, represented as the OID of the counter object in cIscsiTargetLoginStatsTable for which the relevant instance was incremented. A value of 0.0 indicates a type which is not represented by any of the counters in cIscsiTargetLoginStatsTable.
cIscsiTgtLastIntrFailureName	An octet string giving the name of the initiator that failed the last login attempt.
cIscsiTgtLastIntrFailureAddr	An Internet Network Address giving the host address of the initiator that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

Trap: ciscoTap2MediationTimedOut

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationTimedOut	Trap	Alarm	Yes	Normal	$NodeDisplayName - Tap2Mediation status is active.	Tap2MediationTimedOut	PDNGW
Tap2MediationTimedOut	Trap	Alarm	Yes	Critical	$NodeDisplayName - Tap2Mediation status is notInService.	Tap2MediationTimedOut	PDNGW
Tap2MediationTimedOut	Trap	Alarm	Yes	Warning	$NodeDisplayName - Tap2Mediation status is notReady.	Tap2MediationTimedOut	PDNGW
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndGo.	Tap2MediationTimedOut	PDNGW
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndWait.	Tap2MediationTimedOut	PDNGW
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is destroy.	Tap2MediationTimedOut	PDNGW

Description:

```
When an intercept is autonomously removed by an intercepting       device, such as due to the time specified in
cTap2MediationTimeout arriving, the device notifies the manager
of the action.
```

Default Message:

$NodeDisplayName - Tap2Mediation status is active.
$NodeDisplayName - Tap2Mediation status is notReady.
$NodeDisplayName - Tap2Mediation status is notInService.
$NodeDisplayName - Tap2Mediation status is createAndGo.
$NodeDisplayName - Tap2Mediation status is createAndWait.
$NodeDisplayName - Tap2Mediation status is destroy.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2MediationStatus	The status of this conceptual row. This object is used to manage creation, modification and deletion of rows in this table. cTap2MediationTimeout may be modified at any time (even while the row is active). But when the row is active, the other writable objects may not be modified without setting its value to 'notInService'. The entry may not be deleted or deactivated by setting its value to 'destroy' or 'notInService' if there is any associated entry in cTap2StreamTable. The RowStatus textual convention is used to manage the creation and deletion of conceptual rows, and is used as the value of the SYNTAX clause for the status column of a conceptual row (as described in Section 7.7.1 of [2].) The status column has six defined values: - `active', which indicates that the conceptual row is available for use by the managed device; - `notInService', which indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device (see NOTE below); - `notReady', which indicates that the conceptual row exists in the agent, but is missing information necessary in order to be available for use by the managed device; - `createAndGo', which is supplied by a management station wishing to create a new instance of a conceptual row and to have its status automatically set to active, making it available for use by the managed device; - `createAndWait', which is supplied by a management

station wishing to create a new instance of a
conceptual row (but not make it available for use by
the managed device); and,
- `destroy', which is supplied by a management station
wishing to delete all of the instances associated with
an existing conceptual row.
Whereas five of the six values (all except `notReady') may
be specified in a management protocol set operation, only
three values will be returned in response to a management
protocol retrieval operation: `notReady', `notInService' or
`active'. That is, when queried, an existing conceptual row
has only three states: it is either available for use by
the managed device (the status column has value `active');
it is not available for use by the managed device, though
the agent has sufficient information to make it so (the
status column has value `notInService'); or, it is not
available for use by the managed device, and an attempt to
make it so would fail because the agent has insufficient
information (the state column has value `notReady').
NOTE WELL
This textual convention may be used for a MIB table,
irrespective of whether the values of that table's
conceptual rows are able to be modified while it is
active, or whether its conceptual rows must be taken
out of service in order to be modified. That is, it is
the responsibility of the DESCRIPTION clause of the
status column to specify whether the status column must
not be `active' in order for the value of some other
column of the same conceptual row to be modified. If
such a specification is made, affected columns may be
changed by an SNMP set PDU if the RowStatus would not
be equal to `active' either immediately before or after
processing the PDU. In other words, if the PDU also
contained a varbind that would change the RowStatus
value, the column in question may be changed if the
RowStatus was not equal to `active' as the PDU was
received, or if the varbind sets the status to a value
other than 'active'.
Also note that whenever any elements of a row exist, the
RowStatus column must also exist.
To summarize the effect of having a conceptual row with a
status column having a SYNTAX clause value of RowStatus,
consider the following state diagram:
STATE
+--------------+-----------+-------------+-------------
| A | B | C | D
| |status col.|status column|
|status column | is | is |status column
ACTION |does not exist| notReady | notInService| is active
--------------+--------------+-----------+-------------+-------------
set status |noError ->D|inconsist- |inconsistent-|inconsistent-
column to | or | entValue| Value| Value
createAndGo |inconsistent- | | |
| Value| | |
--------------+--------------+-----------+-------------+-------------
set status |noError see 1|inconsist- |inconsistent-|inconsistent-
column to | or | entValue| Value| Value
createAndWait |wrongValue | | |
--------------+--------------+-----------+-------------+-------------
set status |inconsistent- |inconsist- |noError |noError
column to | Value| entValue| |
active | | | |
| | or | |
| | | |
| |see 2 ->D| ->D| ->D
--------------+--------------+-----------+-------------+-------------
set status |inconsistent- |inconsist- |noError |noError ->C
column to | Value| entValue| |
notInService | | | |
| | or | | or
| | | |

| |see 3 ->C| ->C|wrongValue
---|---|---|---|---
set status |noError |noError |noError |noError
column to | | | |
destroy	->A	->A	->A	->A
set any other |see 4 |noError |noError |see 5
column to some			
value		see 1	->C	->D

(1) goto B or C, depending on information available to the agent.
(2) if other variable bindings included in the same PDU, provide values for all columns which are missing but required, then return noError and goto D.
(3) if other variable bindings included in the same PDU, provide values for all columns which are missing but required, then return noError and goto C.
(4) at the discretion of the agent, the return value may be either:
inconsistentName: because the agent does not choose to create such an instance when the corresponding RowStatus instance does not exist, or
inconsistentValue: if the supplied value is inconsistent with the state of some other MIB object's value, or
noError: because the agent chooses to create the instance.
If noError is returned, then the instance of the status column must also be created, and the new state is B or C, depending on the information available to the agent. If inconsistentName or inconsistentValue is returned, the row remains in state A.
(5) depending on the MIB definition for the column/table, either noError or inconsistentValue may be returned.
NOTE: Other processing of the set request may result in a response other than noError being returned, e.g., wrongValue, noCreation, etc.

Conceptual Row Creation

There are four potential interactions when creating a conceptual row: selecting an instance-identifier which is not in use; creating the conceptual row; initializing any objects for which the agent does not supply a default; and, making the conceptual row available for use by the managed device.

Interaction 1: Selecting an Instance-Identifier

The algorithm used to select an instance-identifier varies for each conceptual row. In some cases, the instance-identifier is semantically significant, e.g., the destination address of a route, and a management station selects the instance-identifier according to the semantics.

In other cases, the instance-identifier is used solely to distinguish conceptual rows, and a management station without specific knowledge of the conceptual row might examine the instances present in order to determine an unused instance-identifier. (This approach may be used, but it is often highly sub-optimal; however, it is also a questionable practice for a naive management station to attempt conceptual row creation.)

Alternately, the MIB module which defines the conceptual row might provide one or more objects which provide assistance in determining an unused instance-identifier. For example, if the conceptual row is indexed by an integer-value, then an object having an integer-valued SYNTAX clause might be defined for such a purpose, allowing a management station to issue a management protocol retrieval operation. In order to avoid unnecessary collisions between competing management stations, `adjacent' retrievals of this object should be different.

Finally, the management station could select a pseudo-random number to use as the index. In the event that this index

was already in use and an inconsistentValue was returned in response to the management protocol set operation, the management station should simply select a new pseudo-random number and retry the operation.

A MIB designer should choose between the two latter algorithms based on the size of the table (and therefore the efficiency of each algorithm). For tables in which a large number of entries are expected, it is recommended that a MIB object be defined that returns an acceptable index for creation. For tables with small numbers of entries, it is recommended that the latter pseudo-random index mechanism be used.

Interaction 2: Creating the Conceptual Row

Once an unused instance-identifier has been selected, the management station determines if it wishes to create and activate the conceptual row in one transaction or in a negotiated set of interactions.

Interaction 2a: Creating and Activating the Conceptual Row

The management station must first determine the column requirements, i.e., it must determine those columns for which it must or must not provide values. Depending on the complexity of the table and the management station's knowledge of the agent's capabilities, this determination can be made locally by the management station. Alternately, the management station issues a management protocol get operation to examine all columns in the conceptual row that it wishes to create. In response, for each column, there are three possible outcomes:

- a value is returned, indicating that some other management station has already created this conceptual row. We return to interaction 1.
- the exception `noSuchInstance' is returned, indicating that the agent implements the object-type associated with this column, and that this column in at least one conceptual row would be accessible in the MIB view used by the retrieval were it to exist. For those columns to which the agent provides read-create access, the `noSuchInstance' exception tells the management station that it should supply a value for this column when the conceptual row is to be created.
- the exception `noSuchObject' is returned, indicating that the agent does not implement the object-type associated with this column or that there is no conceptual row for which this column would be accessible in the MIB view used by the retrieval. As such, the management station can not issue any management protocol set operations to create an instance of this column.

Once the column requirements have been determined, a management protocol set operation is accordingly issued. This operation also sets the new instance of the status column to `createAndGo'.

When the agent processes the set operation, it verifies that it has sufficient information to make the conceptual row available for use by the managed device. The information available to the agent is provided by two sources: the management protocol set operation which creates the conceptual row, and, implementation-specific defaults supplied by the agent (note that an agent must provide implementation-specific defaults for at least those objects which it implements as read-only). If there is sufficient information available, then the conceptual row is created, a `noError' response is returned, the status column is set to `active', and no further interactions are necessary (i.e., interactions 3 and 4 are skipped). If there is insufficient information, then the conceptual row is not created, and the set operation fails with an error of `inconsistentValue'.

On this error, the management station can issue a management protocol retrieval operation to determine if this was because it failed to specify a value for a required column, or, because the selected instance of the status column

already existed. In the latter case, we return to interaction 1. In the former case, the management station can re-issue the set operation with the additional information, or begin interaction 2 again using `createAndWait' in order to negotiate creation of the conceptual row.

NOTE WELL

Regardless of the method used to determine the column requirements, it is possible that the management station might deem a column necessary when, in fact, the agent will not allow that particular columnar instance to be created or written. In this case, the management protocol set operation will fail with an error such as `noCreation' or `notWritable'. In this case, the management station decides whether it needs to be able to set a value for that particular columnar instance. If not, the management station re-issues the management protocol set operation, but without setting a value for that particular columnar instance; otherwise, the management station aborts the row creation algorithm.

Interaction 2b: Negotiating the Creation of the Conceptual Row

The management station issues a management protocol set operation which sets the desired instance of the status column to `createAndWait'. If the agent is unwilling to process a request of this sort, the set operation fails with an error of `wrongValue'. (As a consequence, such an agent must be prepared to accept a single management protocol set operation, i.e., interaction 2a above, containing all of the columns indicated by its column requirements.) Otherwise, the conceptual row is created, a `noError' response is returned, and the status column is immediately set to either `notInService' or `notReady', depending on whether it has sufficient information to make the conceptual row available for use by the managed device. If there is sufficient information available, then the status column is set to `notInService'; otherwise, if there is insufficient information, then the status column is set to `notReady'. Regardless, we proceed to interaction 3.

Interaction 3: Initializing non-defaulted Objects

The management station must now determine the column requirements. It issues a management protocol get operation to examine all columns in the created conceptual row. In the response, for each column, there are three possible outcomes:

- a value is returned, indicating that the agent implements the object-type associated with this column and had sufficient information to provide a value. For those columns to which the agent provides read-create access (and for which the agent allows their values to be changed after their creation), a value return tells the management station that it may issue additional management protocol set operations, if it desires, in order to change the value associated with this column.
- the exception `noSuchInstance' is returned, indicating that the agent implements the object-type associated with this column, and that this column in at least one conceptual row would be accessible in the MIB view used by the retrieval were it to exist. However, the agent does not have sufficient information to provide a value, and until a value is provided, the conceptual row may not be made available for use by the managed device. For those columns to which the agent provides read-create access, the `noSuchInstance' exception tells the management station that it must issue additional management protocol set operations, in order to provide a value associated with this column.
- the exception `noSuchObject' is returned, indicating that the agent does not implement the object-type associated with this column or that there is no

conceptual row for which this column would be
accessible in the MIB view used by the retrieval. As
such, the management station can not issue any
management protocol set operations to create an
instance of this column.
If the value associated with the status column is
`notReady', then the management station must first deal with
all `noSuchInstance' columns, if any. Having done so, the
value of the status column becomes `notInService', and we
proceed to interaction 4.
Interaction 4: Making the Conceptual Row Available
Once the management station is satisfied with the values
associated with the columns of the conceptual row, it issues
a management protocol set operation to set the status column
to `active'. If the agent has sufficient information to
make the conceptual row available for use by the managed
device, the management protocol set operation succeeds (a
`noError' response is returned). Otherwise, the management
protocol set operation fails with an error of
`inconsistentValue'.
NOTE WELL
A conceptual row having a status column with value
`notInService' or `notReady' is unavailable to the
managed device. As such, it is possible for the
managed device to create its own instances during the
time between the management protocol set operation
which sets the status column to `createAndWait' and the
management protocol set operation which sets the status
column to `active'. In this case, when the management
protocol set operation is issued to set the status
column to `active', the values held in the agent
supersede those used by the managed device.
If the management station is prevented from setting the
status column to `active' (e.g., due to management station
or network failure) the conceptual row will be left in the
`notInService' or `notReady' state, consuming resources
indefinitely. The agent must detect conceptual rows that
have been in either state for an abnormally long period of
time and remove them. It is the responsibility of the
DESCRIPTION clause of the status column to indicate what an
abnormally long period of time would be. This period of
time should be long enough to allow for human response time
(including `think time') between the creation of the
conceptual row and the setting of the status to `active'.
In the absense of such information in the DESCRIPTION
clause, it is suggested that this period be approximately 5
minutes in length. This removal action applies not only to
newly-created rows, but also to previously active rows which
are set to, and left in, the notInService state for a
prolonged period exceeding that which is considered normal
for such a conceptual row.
Conceptual Row Suspension
When a conceptual row is `active', the management station
may issue a management protocol set operation which sets the
instance of the status column to `notInService'. If the
agent is unwilling to do so, the set operation fails with an
error of `wrongValue'. Otherwise, the conceptual row is
taken out of service, and a `noError' response is returned.
It is the responsibility of the DESCRIPTION clause of the
status column to indicate under what circumstances the
status column should be taken out of service (e.g., in order
for the value of some other column of the same conceptual
row to be modified).
Conceptual Row Deletion
For deletion of conceptual rows, a management protocol set
operation is issued which sets the instance of the status
column to `destroy'. This request may be made regardless of
the current value of the status column (e.g., it is possible
to delete conceptual rows which are either `notReady',
`notInService' or `active'.) If the operation succeeds,
then all instances associated with the conceptual row are

	immediately removed.
cTap2MediationContentId	cTap2MediationContentId is a session identifier, from the intercept application's perspective, and a content identifier from the Mediation Device's perspective. The Mediation Device is responsible for making sure these are unique, although the SNMP RowStatus row creation process will help by not allowing it to create conflicting entries. Before creating a new entry, a value for this variable may be obtained by reading cTap2MediationNewIndex to reduce the probability of a value collision.

Go Top

SECTION 10.47

Trap: ciscoNtpGeneralConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with all NTP servers is lost	NtpConnectionState	PDNGW
NtpConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with NTP server has been restored	NtpConnectionState	PDNGW

Description:

```
This trap is sent when the device loses connectivity            to all NTP servers.
```

Default Message:

$NodeDisplayName - Connection with all NTP servers is lost.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 10.48

Trap: ciscoNtpHighPriorityConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with the high priority NTP server is failed	NtpHighPriorityConnectionState	PDNGW
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with the high priority NTP server is restored	NtpHighPriorityConnectionState	PDNGW

Description:

```
A failure to connect with an high priority NTP server           (e.g. a server at the lowest stratum) is detected.
```

Default Message:

$NodeDisplayName - Connection with the high priority NTP server is failed

Message Substitution Variables:

Common	Substitution variables common to all traps.
	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpPeersPeerAddress	The IP address of the peer. When creating a new association, a value should be set either for this object or the corresponding instance of cntpPeersPeerName, before the row is made active.
cntpPeersAssocId	An integer value greater than 0 that uniquely identifies a peer with which the local NTP server is associated.

Go Top

SECTION 10.49

Trap: ciscoNtpSrvStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpServerStatus	Trap	Alarm	Yes	Indeterminate	$NodeDisplayName - The NTP server status is unknown	NtpServerStatus	PDNGW
NtpServerStatus	Trap	Alarm	Yes	Critical	$NodeDisplayName - The NTP server is not running	NtpServerStatus	PDNGW
NtpServerStatus	Trap	Alarm	Yes	Warning	$NodeDisplayName - The NTP server is not synchronized to any time source	NtpServerStatus	PDNGW
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to its own local clock	NtpServerStatus	PDNGW
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a local hardware refclock	NtpServerStatus	PDNGW
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a remote NTP server	NtpServerStatus	PDNGW

Description:

```
This notification is generated whenever the value of           cntpSysSrvStatus changes.
```

Default Message:

$NodeDisplayName - The NTP server status is unknown
$NodeDisplayName - The NTP server is not running
$NodeDisplayName - The NTP server is not synchronized to any time source
$NodeDisplayName - The NTP server is synchronized to its own local clock
$NodeDisplayName - The NTP server is synchronized to a local hardware refclock
$NodeDisplayName - The NTP server is synchronized to a remote NTP server

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpSysSrvStatus	Current state of the NTP server with values coded as follows: 1: server status is unknown 2: server is not running 3: server is not synchronized to any time source 4: server is synchronized to its own local clock 5: server is synchronized to a local hardware refclock (e.g. GPS) 6: server is synchronized to a remote NTP server INTEGER is unknown

Go Top

SECTION 10.50

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is above the high threshold of $GGSNHighThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	PDNGW
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	PDNGW
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is below the low threshold of $GGSNLowThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	PDNGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold.

	style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.

width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 10.51

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is above the high threshold of $GGSNHighThreshold percent of total signalling messages received.	GTPUnexpectedMsgsThreshold	PDNGW
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total signalling messages received.	GTPUnexpectedMsgsThreshold	PDNGW
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is below the low threshold of $GGSNLowThreshold percent of the total signalling messages received.	GTPUnexpectedMsgsThreshold	PDNGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This

	alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the

	number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 10.52

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is above the high threshold of $GGSNHighThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	PDNGW

GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	PDNGW
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is below the low threshold of $GGSNLowThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	PDNGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold

	(recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 10.53

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is above the high threshold of $GGSNHighThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	PDNGW
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	PDNGW
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is below the low threshold of $GGSNLowThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	PDNGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289">	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold.

style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 10.54

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is above the high threshold of $GGSNHighThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	PDNGW
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	PDNGW

RejectedPDPContextsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is below the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	PDNGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This

	alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 10.55

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is above the high threshold of $GGSNHighThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	PDNGW
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	PDNGW
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is below the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	PDNGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the

Roman";">IPOutboundNoRoutesThreshold	number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 10.56

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ActiveGTPVersion0PDPsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of active GTP version 0 PDP contexts is $GGSNThresholdValue percent of the active GTP version 0 PDP contexts limit which is above the high threshold of $GGSNHighThreshold percent of the active GTP version 0 PDP contexts limit.	ActiveGTPVersion0PDPsThreshold	PDNGW
ActiveGTPVersion0PDPsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of active GTP version 0 PDP contexts is $GGSNThresholdValue percent of the active GTP version 0 PDP contexts limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the active GTP version 0 PDP contexts limit.	ActiveGTPVersion0PDPsThreshold	PDNGW
ActiveGTPVersion0PDPsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of active GTP version 0 PDP contexts is $GGSNThresholdValue percent of the active GTP version 0 PDP contexts limit which is below the low threshold of $GGSNLowThreshold percent of the active GTP version 0 PDP contexts limit.	ActiveGTPVersion0PDPsThreshold	PDNGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	Alarm Description
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 10.57

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ActiveGTPVersion1PDPsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of active GTP version 1 PDP contexts is $GGSNThresholdValue percent of the active GTP version 1 PDP contexts limit which is above the high threshold of $GGSNHighThreshold percent of the active GTP version 1 PDP contexts limit.	ActiveGTPVersion1PDPsThreshold	PDNGW
ActiveGTPVersion1PDPsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of active GTP version 1 PDP contexts is $GGSNThresholdValue percent of the active GTP version 1 PDP contexts limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the active GTP version 1 PDP contexts limit.	ActiveGTPVersion1PDPsThreshold	PDNGW
ActiveGTPVersion1PDPsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of active GTP version 1 PDP contexts is $GGSNThresholdValue percent of the active GTP version 1 PDP contexts limit which is below the low threshold of $GGSNLowThreshold percent of the active GTP version 1 PDP contexts limit.	ActiveGTPVersion1PDPsThreshold	PDNGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a

	percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 10.58

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is above the high threshold of $GGSNHighThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	PDNGW
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	PDNGW
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is below the low threshold of $GGSNLowThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	PDNGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	Alarm Description
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router

	that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 10.59

Trap: ciscoIpLocalPoolInUseAddrNoti

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	PDNGW
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold abated. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	PDNGW
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	PDNGW

Description:

A notification indicating that number of used addresses of an IP local pool exceeded the threshold value indicated by cIpLocalPoolStatInUseAddrThldHi.

Default Message:

$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIpLocalPoolStatFreeAddrs	The number of IP addresses available for use in this IP local pool.
cIpLocalPoolStatInUseAddrs	The number of IP addresses being used in this IP local pool.

Go Top

SECTION 10.60

Trap: ciscoTap2MIBActive

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MIBActive	Trap	Event	No	Informational	$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.	Tap2MIBActive	PDNGW

Description:

This Notification is sent when an intercepting router or switch is first capable of intercepting a packet corresponding to a configured data stream. The value of the corresponding cTap2StreamType which identifies the actual intercept stream type is included in this notification.
This notification may be generated in conjunction with the intercept application, which is designed to expect the notification to be sent as reliably as possible, e.g., through the use of a finite number of retransmissions until acknowledged, as and when such mechanisms are available; for example, with SNMPv3, this would be an InformRequest. Filter installation can take a long period of time, during which call progress may be delayed.

Default Message:

$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 10.61

Trap: ciscoTap2MediationDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .	Tap2MediationDebug	PDNGW

Description:

When there is intervention needed due to some events related to entries configured in cTap2MediationTable, the device notifies the manager of the event.
This notification may be generated in conjunction with the intercept application, which is designed to expect the notification to be sent as reliably as possible, e.g., through the use of a finite number of retransmissions until acknowledged, as and when such mechanisms are available; for example, with SNMPv3, this would be an InformRequest.

Default Message:

$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 10.62

Trap: ciscoTap2StreamDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2StreamDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId	Tap2StreamDebug	PDNGW

Description:

```
When there is intervention needed due to some events related       to entries configured in cTap2StreamTable, the device
notifies the manager of the event.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.
```

Default Message:

$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId.br>

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.
cTap2DebugStreamId	The value of this object is that of cTap2StreamIndex of an entry in cTap2StreamTable. This object along with cTap2DebugMediationId identifies an entry in cTap2StreamTable. The value of this object may be zero, in which this debug message is regarding a Mediation Device, but not a particular stream. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2StreamTable fails.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 10.63

Trap: ciscoTap2Switchover

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2Switchover	Trap	Event	No	Informational	$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.	Tap2Switchover	PDNGW

Description:

This notification is sent when there is a redundant (standby) route processor available on the intercepting device and the current active processor is going down causing standby to takeover. Note that this notification may be sent by the intercepting device only when it had a chance to know before it goes down.
Mediation device when received this notification should assume that configured intercepts on the intercepting device no longer exist, when the standby processor takes control. This means that the Mediation device should again configure the intercepts.

Default Message:

$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 10.64

Status: ApnInstanceStateAdded and ApnInstanceStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceState	Poll	Event	No	Normal	APN $ApnDisplayName on gateway $NodeDisplayName added in state Active/ActiveReason.	ApnInstanceState	PDNGW
ApnInstanceState	Poll	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName added in state $ApnInstanceState/$ApnInstanceStateReason.	ApnInstanceState	PDNGW
ApnInstanceState	Poll	Event	No	Normal	APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to Active/ActiveReason.	ApnInstanceState	PDNGW
ApnInstanceState	Poll	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to $ApnInstanceState/$ApnInstanceStateReason.	ApnInstanceState	PDNGW

Description:

The ApnInstanceStateAdded and ApnInstanceStateChanged status eventsprovide information when an ApnInstance object is added to the MWTM object model or when MWTM detects that the state of an ApnInstance has changed. An ApnInstance is defined as an access-point and accesspoint-name defined on a gateway router. An ApnInstance object is located under the gateway Node object in the MWTM object tree. The value of ApnInstanceState indicates the new state. Possible values of ApnInstanceState include:

- Active - Traffic may flow over this ApnInstance.
- Unknown - The attempt to determine the state of the ApnInstance failed.
- Warning - The ApnInstance is Active however some underlying status contributor of this ApnInstance is not fully functional.
- Deleted - The ApnInstance has been deleted from the object database.

Default Message:

- APN $ApnDisplayName on gateway $NodeDisplayName added in state $ApnInstanceState/$ApnInstanceStateReason.
- APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to $ApnInstanceState/$ApnInstanceStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.

ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
ApnInstanceState	The current state of the ApnInstance.
ApnInstanceStateReason	The current state reason of of the ApnInstance.
ApnInstanceLastState	The previous state of the ApnInstance.

Operational Information:

See also:

Go Top

SECTION 10.65

Status: ApnStateAdded and ApnStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnState	Poll	Event	No	Normal	APN $ApnDisplayName added in state Active/ActiveReason.	ApnState	PDNGW
ApnState	Poll	Event	No	Informational	APN $ApnDisplayName added in state $ApnState/$ApnStateReason.	ApnState	PDNGW
ApnState	Poll	Event	No	Normal	APN $ApnDisplayName changed state from $ApnLastState to Active/ActiveReason.	ApnState	PDNGW
ApnState	Poll	Event	No	Informational	APN $ApnDisplayName changed state from $ApnLastState to $ApnState/$ApnStateReason.	ApnState	PDNGW

Description:

The ApnStateAdded and ApnStateChanged status events provideinformation when an Apn object is added to the MWTM object model or when MWTM detects that the state of an Apn has changed. An Apn is defined as an aggregation of a set of ApnInstance objects defined across a set of gateway routers. An Apn object is located as a top level object in the MWTM object tree. The value of ApnState indicates the new state.
Possible values of ApnState include:

- Active - Traffic may flow over this Apn.
- Warning - The Apn is Active however one or more of its constituent ApnInstances is not fully functional.
- Deleted - The Apn has been deleted from the object database.

Default Message:

- Apn $ApnDisplayName added in state $ApnState/$ApnStateReason.
- Apn $ApnDisplayName changed state from $ApnLastState to $ApnState/$ApnStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
ApnState	The current state of the Apn.
ApnStateReason	The current state reason of of the Apn.
ApnLastState	The previous state of the Apn.

Operational Information:

See also:

Go Top

SECTION 10.66

UserAction: ApnInstanceIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceIgnoredSet	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.	ApnInstanceIgnoredSet	PDNGW

Description:

The ApnInstanceIgnoredSet UserAction event provides information when a ApnInstance's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the ApnInstance in the aggregation algorithm in determining the state of a Node or Apn. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The ApnInstance is to be excluded from state aggregation.
- False - The ApnInstance is to be included in state aggregation.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
ApnInstanceState	The current state of the ApnInstance.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the ApnInstances which are currently ignored select the ApnInstance folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 10.67

UserAction: ApnIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnIgnoredSet	User Action	Event	No	Informational	APN $ApnDisplayName ignore flag is set to $IgnoredFlag by $User.	ApnIgnoredSet	PDNGW

Description:

The ApnIgnoredSet UserAction event provides information when a Apn's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the Apn in the aggregation algorithm in determining the state of higher level objects. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The Apn is to be excluded from state aggregation.
- False - The Apn is to be included in state aggregation.

Default Message:

APN $ApnDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
ApnState	The current state of the Apn.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the Apns which are currently ignored select the Apn folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 10.68

UserAction: ApnInstanceUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceUserDataUpdated	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName edited by user $User.	ApnInstanceUserDataUpdated	PDNGW

Description:

The ApnInstanceUserDataUpdated UserAction event provides information when a ApnInstance object's user data has been updated by a MWTM user.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName edited by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
User	The user who requested the ApnInstance's data be updated.

Operational Information:

The fields that can be updated for a ApnInstance include:

- The ApnInstance's notes data used for communicating installation dependent information about a ApnInstance.

Go Top

SECTION 10.69

UserAction: ApnUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnUserDataUpdated	User Action	Event	No	Informational	APN $ApnDisplayName edited by user $User.	ApnUserDataUpdated	PDNGW

Description:

The ApnUserDataUpdated UserAction event provides information when a Apn object's user data has been updated by a MWTM user.

Default Message:

APN $ApnDisplayName edited by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
User	The user who requested the Apn's data be updated.

Operational Information:

The fields that can be updated for a Apn include:

- The Apn's notes data used for communicating installation dependent information about a Apn.

Go Top

SECTION 10.70

UserAction: ApnInstanceDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceDeleted	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName deleted by user $User.	ApnInstanceDeleted	PDNGW

Description:

The ApnInstanceDeleted UserAction event provides information when a ApnInstanceobject's deletion from the MWTM object model database is requested.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName deleted by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
User	The user who requested the ApnInstance's data be deleted.

Operational Information:

- The deletion of a ApnInstance can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 10.71

UserAction: ApnDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnDeleted	User Action	Event	No	Informational	APN $ApnDisplayName deleted by user $User.	ApnDeleted	PDNGW

Description:

The ApnDeleted UserAction event provides information when a Apnobject's deletion from the MWTM object model database is requested.

Default Message:

APN $ApnDisplayName deleted by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
User	The user who requested the Apn's data be deleted.

Operational Information:

- The deletion of a Apn can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 11.1

Trap: cCdmaClusterCtrlStatusChange2

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ClusterControlState	Trap	Alarm	Yes	Warning	$NodeDisplayName - The gateway cluster member reports that the cluster controller status as notConfigured.	ClusterControlState	PDSN
ClusterControlState	Trap	Event	Yes	Informational	$NodeDisplayName - The cCdmaClusterCtrlStatusChange trap is deprecated.	ClusterControlState	PDSN
ClusterControlState	Trap	Alarm	Yes	Warning	$NodeDisplayName - The gateway cluster member reports that the cluster controller status as configured.	ClusterControlState	PDSN
ClusterControlState	Trap	Alarm	Yes	Normal	$NodeDisplayName - The gateway cluster member reports that the cluster controller status alive.	ClusterControlState	PDSN
ClusterControlState	Poll	Alarm	Yes	Warning	$NodeDisplayName - The gateway cluster member reports that the cluster controller status as configured.	ClusterControlState	PDSN
ClusterControlState	Poll	Alarm	Yes	Normal	$NodeDisplayName - The gateway cluster member reports that the cluster controller status as alive.	ClusterControlState	PDSN
ClusterControlState	Poll	Alarm	Yes	Warning	$NodeDisplayName - The gateway cluster member reports that the cluster controller status as notConfigured.	ClusterControlState	PDSN

Description:

```
Cluster member PDSN detects controller PDSN status                change
```

Default Message:

$NodeDisplayName - The gateway cluster member reports as not configured.
$NodeDisplayName - The gateway cluster member reports that the cluster controller as configured.
$NodeDisplayName - The gateway cluster member reports that the cluster controller is alive.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cCdmaClusterCtrlStatus	The operational status of the cluster controller maintained by the member. INTEGER is unknown

cCdmaClusterCtrlAddress	This is the IP address of a particular controller and is used as index (combine with cCdmaCluster-CtrlAddressType) to identify a unique cluster controller entry.
cCdmaClusterCtrlAddressType	This is the IP address type of a particular controller and is used as index (combine with cCdmaClusterCtrlAddress) to identify a unique cluster controller entry.

Go Top

SECTION 11.2

Trap: cCdmaClusterMemberStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ClusterMemberState	Trap	Event	Yes	Informational	$NodeDisplayName - The cCdmaClusterMemberStatusChange is deprecated.	ClusterMemberState	PDSN
ClusterMemberState	Trap	Alarm	Yes	Major	$NodeDisplayName - The gateway cluster controller reports that the status of cluster member is unknown.	ClusterMemberState	PDSN
ClusterMemberState	Trap	Alarm	Yes	Normal	$NodeDisplayName - The gateway cluster controller reports that the status of cluster member is ready.	ClusterMemberState	PDSN
ClusterMemberState	Trap	Alarm	Yes	Major	$NodeDisplayName - The gateway cluster controller reports that the status of cluster member is adminProhibit.	ClusterMemberState	PDSN
ClusterMemberState	Poll	Alarm	Yes	Warning	$NodeDisplayName - The gateway cluster controller reports that the status of cluster member $cCdmaAffectedAddress is ready..	ClusterMemberState	PDSN
ClusterMemberState	Poll	Alarm	Yes	Warning	$NodeDisplayName - The gateway cluster controller reports that the status of cluster member $cCdmaAffectedAddress is administratively prohibited. New calls will not be accepted by this cluster member..	ClusterMemberState	PDSN
ClusterMemberState	Poll	Alarm	Yes	Warning	$NodeDisplayName - The gateway cluster controller reports that the status of cluster member $cCdmaAffectedAddress is unknown..	ClusterMemberState	PDSN

Description:

```
Cluster controller detects member PDSN status                  change
```

Default Message:

$NodeDisplayName - The cCdmaClusterMemberStatusChange is deprecated.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cCdmaServiceAffectedLevel	This is the severity level of affected service by this event/condition that causes this notification. CDMA severity level of affected service: - 'warning' indicates something is abnormal, but service is not affected. - 'minor' indicates service has been slightly affected. - 'major' indicates service has been severely affected. - 'critical' indicates service can not be provided anymore.
cCdmaAffectedAddressType	This is the IP address type of affected device that generates this notification.

	A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cCdmaAffectedMemberStatus	The operational status of affected member PDSN. INTEGER is unknown
cCdmaAffectedAddress	This is the IP address of affected device that generates this notification.

Go Top

SECTION 11.3

Trap: cCdmaClusterSessionLowReached

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ClusterSessionThreshold	Trap	Alarm	Yes	Minor	$NodeDisplayName - The gateway cluster controller session low threshold has been reached. Low threshold: $cCdmaClusterSessLowThreshold	ClusterSessionThreshold	PDSN
ClusterSessionThreshold	Trap	Alarm	Yes	Major	$NodeDisplayName - The gateway cluster controller session high threshold has been reached. High threshold: $cCdmaClusterSessHighThreshold	ClusterSessionThreshold	PDSN
ClusterSessionThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The gateway cluster controller session high threshold has been reached. High threshold: $cCdmaClusterSessHighThreshold	ClusterSessionThreshold	PDSN
ClusterSessionThreshold	Poll	Alarm	Yes	Minor	$NodeDisplayName - The gateway cluster controller session low threshold has been reached. Low threshold: $cCdmaClusterSessLowThreshold	ClusterSessionThreshold	PDSN
ClusterSessionThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The gateway cluster controller session low threshold has been reached. Low threshold: $cCdmaClusterSessLowThreshold	ClusterSessionThreshold	PDSN

Description:

```
This notification indicates a cluster session                  low threshold has been reached by PDSN cluster
controller.
Service affected level: Major/Warning
```

Default Message:

$NodeDisplayName - The gateway cluster controller session low threshold has been reached. Low threshold: $cCdmaClusterSessLowThreshold

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cCdmaServiceAffectedLevel	This is the severity level of affected service by this event/condition that causes this notification. CDMA severity level of affected service: - 'warning' indicates something is abnormal, but service is not affected. - 'minor' indicates service has been slightly affected. - 'major' indicates service has been severely affected. - 'critical' indicates service can not be provided anymore.
cCdmaClusterSessLowThreshold	A threshold marking the low number of allowed sessions within a PDSN cluster controller. Notification will be generated when this threshold is reached during call release.

Go Top

SECTION 11.4

Trap: cCdmaPcfMaxAllowedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PCF-Threshold	Trap	Alarm	Yes	Critical	$NodeDisplayName - The gateway has reached the maximum number of base station controller-packet control functions allowed. Requests from new PCFs will be rejected. Max allowed: $cCdmaPcfMaxAllowed.	PCF-Threshold	PDSN
PCF-Threshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The gateway base station controller-packet control functions count is below the maximum allowed. Max allowed: $cCdmaPcfMaxAllowed	PCF-Threshold	PDSN
PCF-Threshold	Poll	Alarm	Yes	Critical	$NodeDisplayName - The gateway has reached the maximum number of base station controller-packet control functions allowed. Requests from new PCFs will be rejected. Max allowed: $cCdmaPcfMaxAllowed.	PCF-Threshold	PDSN

Description:

```
This notification indicates PDSN has reached the                maximum number of allowed PCF. In this state
request from new PCF will be rejected.
Service affected level: critical
```

Default Message:

$NodeDisplayName - The gateway has reached the maximum number of base station controller-packet control functions allowed. Requests from new PCFs will be rejected. Max allowed: $cCdmaPcfMaxAllowed

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cCdmaPcfMaxAllowed	The maximum number of PCF allowed by this system.

Go Top

SECTION 11.5

Trap: cCdmaSessionHighReached

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SessionThreshold	Trap	Alarm	Yes	Major	$NodeDisplayName - The gateway session high threshold has been reached. High threshold: $cCdmaSessionHighThreshold	SessionThreshold	PDSN
SessionThreshold	Trap	Event	Yes	Informational	$NodeDisplayName - The cCdmaSessionLowReached notification is deprecated.	SessionThreshold	PDSN
SessionThreshold	Trap	Alarm	Yes	Critical	$NodeDisplayName - The gateway has reached the maximum number of sessions allowed. New sessions will be rejected. Max allowed: $cCdmaSessionMaxAllowed	SessionThreshold	PDSN
SessionThreshold	Trap	Alarm	Yes	Minor	$NodeDisplayName - The gateway session low threshold has been reached. Low threshold: $cCdmaSessionLowThreshold	SessionThreshold	PDSN
SessionThreshold	Poll	Alarm	Yes	Minor	$NodeDisplayName - The gateway session low threshold has been reached. Low threshold: $cCdmaSessionLowThreshold	SessionThreshold	PDSN
SessionThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The gateway session count is below the low threshold. Low threshold: $cCdmaSessionLowThreshold	SessionThreshold	PDSN
SessionThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The gateway session high threshold has been reached. High threshold: $cCdmaSessionHighThreshold	SessionThreshold	PDSN
SessionThreshold	Poll	Alarm	Yes	Critical	$NodeDisplayName - The gateway has reached the maximum number of sessions allowed. New sessions will be rejected. Max allowed: $cCdmaSessionMaxAllowed	SessionThreshold	PDSN

Description:

```
This notification indicates a session high                    threshold has been has been reached.
```

Default Message:

$NodeDisplayName - The gateway session high threshold has been reached. High threshold: $cCdmaSessionHighThreshold

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cCdmaServiceAffectedLevel	This is the severity level of affected service by this event/condition that causes this notification. CDMA severity level of affected service: - 'warning' indicates something is abnormal, but service is not affected. - 'minor' indicates service has been slightly affected. - 'major' indicates service has been severely affected. - 'critical' indicates service can not be provided anymore.
cCdmaSessionHighThreshold	A threshold marking the high number of allowed sessions. Agent generates a notification when this threshold is reached during call setup.

Go Top

SECTION 11.6

Trap: ciscoCdmaExtLoadHighReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
BandwithUsageThreshold	Trap	Alarm	Yes	Critical	$NodeDisplayName - The gateway bandwidth high threshold has been reached.	BandwithUsageThreshold	PDSN

BandwithUsageThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName - The gateway bandwidth low threshold has been reached.	BandwithUsageThreshold	PDSN

Description:

```
A notification of this type is generated by PDSN                    to indicated that PDSN has exceeds the maximum
load configured.
Maximum load on PDSN is based on the any one of
following parameters bandwidth, cputhreshold,
procmemthreshold and iomemthreshold
The notification reason object indicates the parameter
that has exceeds the configured load.
```

Default Message:

$NodeDisplayName - The gateway bandwidth high threshold has been reached.
$NodeDisplayName - The gateway CPU usage high threshold has been reached.
$NodeDisplayName - The gateway process memory usage high threshold has been reached.
$NodeDisplayName - The gateway IO memory usage high threshold has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccpCdmaExtNotifReason	This object indicates the notification causes for the maximum load notification generated by the PDSN. The notification causes for the maximum load notification are as follows : ` 'bandwidth' - Allowed bandwidth limit reached 'cputhreshold' - Allowed CPU threshold limit reached 'procthreshold' - Allowed process memory limit reached 'iomemthreshold' - Allowed i/o memory limit reached. INTEGER is unknown
cCdmaServingPdsnHostname	Hostname of the serving PDSN.
ccpCdmaExtNotifReasonCurrentValue	This object indicates current value of ccpCdmaExtNotifReason.

Go Top

SECTION 11.7

Trap: cCdmaPdsnStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
PDSN-SystemStatus	Trap	Alarm	Yes	Critical	$NodeDisplayName - The gateway system status is down.	PDSN-SystemStatus	PDSN
PDSN-SystemStatus	Trap	Alarm	Yes	Critical	$NodeDisplayName - The gateway system status indicates insufficient resources to continue normal operations.	PDSN-SystemStatus	PDSN
PDSN-SystemStatus	Trap	Alarm	Yes	Minor	$NodeDisplayName - The gateway system status is unknown.	PDSN-SystemStatus	PDSN
PDSN-SystemStatus	Trap	Alarm	Yes	Warning	$NodeDisplayName - The gateway system status is testing mode. Calls are not accepted via the A10/A11 interface.	PDSN-SystemStatus	PDSN
PDSN-SystemStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The gateway system status is up and providing normal service.	PDSN-SystemStatus	PDSN
PDSN-SystemStatus	Poll	Alarm	Yes	Critical	$NodeDisplayName - The gateway system status is down.	PDSN-SystemStatus	PDSN
PDSN-	Poll	Alarm	Yes	Critical	$NodeDisplayName - The gateway system status indicates insufficient resources to continue normal	PDSN-	PDSN

SystemStatus					operations.	SystemStatus	
PDSN-SystemStatus	Poll	Alarm	Yes	Minor	$NodeDisplayName - The gateway system status is unknown.	PDSN-SystemStatus	PDSN
PDSN-SystemStatus	Poll	Alarm	Yes	Warning	$NodeDisplayName - The gateway system status is testing mode. Calls are not accepted via the A10/A11 interface.	PDSN-SystemStatus	PDSN
PDSN-SystemStatus	Poll	Alarm	Yes	Normal	$NodeDisplayName - The gateway system status is up and providing normal service.	PDSN-SystemStatus	PDSN

Description:

```
This notification indicates status change of PDSN.
```

Default Message:

$NodeDisplayName - The gateway system status is down.
$NodeDisplayName - The gateway system status indicates insufficient resources to continue normal operations.
$NodeDisplayName - The gateway system status is unknown.
$NodeDisplayName - The gateway system status is testing mode. Calls are not accepted via the A10/A11 interface.
$NodeDisplayName - The gateway system status is up and providing normal service.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cCdmaServiceAffectedLevel	This is the severity level of affected service by this event/condition that causes this notification. CDMA severity level of affected service: - 'warning' indicates something is abnormal, but service is not affected. - 'minor' indicates service has been slightly affected. - 'major' indicates service has been severely affected. - 'critical' indicates service can not be provided anymore.
cCdmaSystemStatus	PDSN subsystem operational status. PDSN operational status. The valid value are: - 'unknown' indicates status is unknown. - 'up' indicates system is up and providing service. - 'down' indicates system is down and not providing service. - 'testing' indicates system is up, but is in testing state, call can only be made through CLI, not through regular through A11/A10 interface. - 'insufficientResources' indicates system is up and runs out of system resource.

Go Top

SECTION 11.8

Trap: cCdmaSessionFormatErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SessionFormatError	Trap	Alarm	No	Informational	$NodeDisplayName - This notification is obsolete. The gateway received invalid arguments from a base station controller-packet control function leading to a session termination.	SessionFormatError	PDSN

Description:

```
  This notification indicates PDSN received                    invalid
arguments from PCF leading to session termination.
The agent should not generate more than 1 trap
  of this
type per second to minimize the level of
  management
traffic on the network
```

Default Message:

$NodeDisplayName - This notification is obsolete. The gateway received invalid arguments from a base station controller-packet control function leading to a session termination.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cCdmaFailSessionMsid	MSID of the mobile station for the failed session.
cCdmaFailSessionA11HaIp	MoIP Home Agent address on the A11 interface for the failed session.
cCdmaFailSessionA11FaIp	MoIP Foreign Agent address on the A11 interface for the failed session.
cCdmaFailSessionConnId	Connection ID of the failed session.
cCdmaFailSessionIndex	An arbitrary integer to uniquely identify this entry. Increases monotonically then wrap to zero.

Go Top

SECTION 11.9

Trap: cCdmaSessionRegReqFailedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SessionRegistrationRequestFailed	Trap	Alarm	No	Warning	$NodeDisplayName - The gateway received a registration request that failed due to $cCdmaFailHistFailType.	SessionRegistrationRequestFailed	PDSN

Description:

```
This notification indicates a Registration                   Request received has failed which may be due to
one of the following reasons:
    insufficient resource,
    Administrative prohibition,
    MN authentication failure,
    registration id mismatch,
    bad request,
    unknown HA address
    or T  bit not set or unsupported VID.
The agent should not generate more than 1 trap
of same type per second to minimize the level of
management traffic on the network.
Service affected level: minor
```

Default Message:

$NodeDisplayName - The gateway received a registration request that failed due to $cCdmaFailHistFailType.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cCdmaFailHistFailType	Type of failure for the current record. INTEGER is unknown
cCdmaFailSessionMsid	MSID of the mobile station for the failed session.
cCdmaFailSessionA11HaIp	MoIP Home Agent address on the A11 interface for the failed session.
cCdmaFailSessionA11FaIp	MoIP Foreign Agent address on the A11 interface for the failed session.
cCdmaFailSessionConnId	Connection ID of the failed session.
cCdmaFailSessionIndex	An arbitrary integer to uniquely identify this entry. Increases monotonically then wrap to zero.

Go Top

SECTION 11.10

Trap: ciscoCdmaExtLoadHighReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CPUUsageThreshold	Trap	Alarm	Yes	Critical	$NodeDisplayName - The gateway CPU usage high threshold has been reached.	CPUUsageThreshold	PDSN
CPUUsageThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName - The gateway CPU usage low threshold has been reached.	CPUUsageThreshold	PDSN

Description:

```
A notification of this type is generated by PDSN                    to indicated that PDSN has exceeds the maximum
load configured.
Maximum load on PDSN is based on the any one of
following parameters bandwidth, cputhreshold,
procmemthreshold and iomemthreshold
The notification reason object indicates the parameter
that has exceeds the configured load.
```

Default Message:

$NodeDisplayName - The gateway bandwidth high threshold has been reached.
$NodeDisplayName - The gateway CPU usage high threshold has been reached.
$NodeDisplayName - The gateway process memory usage high threshold has been reached.
$NodeDisplayName - The gateway IO memory usage high threshold has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccpCdmaExtNotifReason	This object indicates the notification causes for the maximum load notification generated by the PDSN. The notification causes for the maximum load notification are as follows : ` 'bandwidth' - Allowed bandwidth limit reached 'cputhreshold' - Allowed CPU threshold limit reached 'procthreshold' - Allowed process memory limit reached 'iomemthreshold' - Allowed i/o memory limit reached. INTEGER is unknown

cCdmaServingPdsnHostname	Hostname of the serving PDSN.
ccpCdmaExtNotifReasonCurrentValue	This object indicates current value of ccpCdmaExtNotifReason.

Go Top

SECTION 11.11

Trap: ciscoCdmaExtLoadHighReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ProcessMemoryUsageThreshold	Trap	Alarm	Yes	Critical	$NodeDisplayName - The gateway process memory usage high threshold has been reached.	ProcessMemoryUsageThreshold	PDSN
ProcessMemoryUsageThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName - The gateway process memory usage low threshold has been reached.	ProcessMemoryUsageThreshold	PDSN

Description:

```
A notification of this type is generated by PDSN                    to indicated that PDSN has exceeds the maximum
load configured.
Maximum load on PDSN is based on the any one of
following parameters bandwidth, cputhreshold,
procmemthreshold and iomemthreshold
The notification reason object indicates the parameter
that has exceeds the configured load.
```

Default Message:

$NodeDisplayName - The gateway bandwidth high threshold has been reached.
$NodeDisplayName - The gateway CPU usage high threshold has been reached.
$NodeDisplayName - The gateway process memory usage high threshold has been reached.
$NodeDisplayName - The gateway IO memory usage high threshold has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccpCdmaExtNotifReason	This object indicates the notification causes for the maximum load notification generated by the PDSN. The notification causes for the maximum load notification are as follows : ` 'bandwidth' - Allowed bandwidth limit reached 'cputhreshold' - Allowed CPU threshold limit reached 'procthreshold' - Allowed process memory limit reached 'iomemthreshold' - Allowed i/o memory limit reached. INTEGER is unknown
cCdmaServingPdsnHostname	Hostname of the serving PDSN.
ccpCdmaExtNotifReasonCurrentValue	This object indicates current value of ccpCdmaExtNotifReason.

Go Top

SECTION 11.12

Trap: ciscoCdmaExtLoadHighReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IOMemoryUsageThreshold	Trap	Alarm	Yes	Critical	$NodeDisplayName - The gateway IO memory usage high threshold has been reached.	IOMemoryUsageThreshold	PDSN

IOMemoryUsageThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName - The gateway IO memory usage low threshold has been reached.	IOMemoryUsageThreshold	PDSN

Description:

```
A notification of this type is generated by PDSN                    to indicated that PDSN has exceeds the maximum
load configured.
Maximum load on PDSN is based on the any one of
following parameters bandwidth, cputhreshold,
procmemthreshold and iomemthreshold
The notification reason object indicates the parameter
that has exceeds the configured load.
```

Default Message:

$NodeDisplayName - The gateway bandwidth high threshold has been reached.
$NodeDisplayName - The gateway CPU usage high threshold has been reached.
$NodeDisplayName - The gateway process memory usage high threshold has been reached.
$NodeDisplayName - The gateway IO memory usage high threshold has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
ccpCdmaExtNotifReason	This object indicates the notification causes for the maximum load notification generated by the PDSN. The notification causes for the maximum load notification are as follows : ` 'bandwidth' - Allowed bandwidth limit reached 'cputhreshold' - Allowed CPU threshold limit reached 'procthreshold' - Allowed process memory limit reached 'iomemthreshold' - Allowed i/o memory limit reached. INTEGER is unknown
cCdmaServingPdsnHostname	Hostname of the serving PDSN.
ccpCdmaExtNotifReasonCurrentValue	This object indicates current value of ccpCdmaExtNotifReason.

Go Top

SECTION 11.13

Trap: cCdmaAhdlcEngineDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
AHDLCEngineState	Trap	Alarm	Yes	Major	$NodeDisplayName - The gateway AHDLC engine is $cCdmaAhdlcEngineAdminState.	AHDLCEngineState	PDSN
AHDLCEngineState	Poll	Alarm	Yes	Major	$NodeDisplayName - The gateway AHDLC engine $cCdmaAhdlcEngineName is down.	AHDLCEngineState	PDSN
AHDLCEngineState	Poll	Alarm	Yes	Warning	$NodeDisplayName - The gateway AHDLC engine $cCdmaAhdlcEngineName is administratively down.	AHDLCEngineState	PDSN
AHDLCEngineState	Poll	Alarm	Yes	Normal	$NodeDisplayName - The gateway AHDLC engine $cCdmaAhdlcEngineName is up.	AHDLCEngineState	PDSN

Description:

```
This notification indicates an AHDLC engine                is 'down' due to some fault though the desired
state of the engine is 'up'.
```

Default Message:

$NodeDisplayName - The gateway AHDLC engine $cCdmaAhdlcEngineName is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cCdmaAhdlcEngineOperState	This object defines the current AHDLC engine operational state. The 'up' indicates the engine is ready to receive ahdlc packets. If cCdmaAhdlcEngineAdminState is 'down' then cCdmaAhdlcEngineOperState should be 'down'. If cCdmaAhdlcEngineAdminState is changed to 'up' then cCdmaAhdlcEngineOperState should change to 'up' if the engine is ready to receive ahdlc packets; it should remain in the 'down' state if and only if there is a fault that prevents it from going to the 'up' state. INTEGER is unknown
cCdmaAhdlcEngineAdminState	This object defines the AHDLC engine desired state. When a managed system initializes, all interfaces start with 'down' state. As a result of either explicit management action or per configuration information retained by the managed system, cCdmaAhdlcEngineAdminState is then changed to either 'up' or remains in the 'down' state. INTEGER is unknown
cCdmaAhdlcEngineIndex	An arbitrary non-zero integer-value that uniquely identifies an AHDLC engine. An implementation should assign AHDLC engines consecutive monotonically increasing values.

Go Top

SECTION 11.14

Trap: cvpdnNotifSession

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
VPDNSessionState	Trap	Event	No	Normal	$NodeDisplayName - The VPDN session is up: Session Id: $cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID.	VPDNSessionState	PDSN
VPDNSessionState	Trap	Event	No	Warning	$NodeDisplayName - The VPDN session is down: Session Id: $cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID	VPDNSessionState	PDSN

Description:

```
Conveys an event regarding the L2X session with the indicated session ID and Xconnect VCID.
```

Default Message:

$NodeDisplayName - The VPDN session is down: Session Id: $ cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID
$NodeDisplayName - The VPDN session is up: Session Id: $ cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID
$NodeDisplayName - The VPDN session pseudowire is down: Session Id: $ cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID
$NodeDisplayName - The VPDN session pseudowire is up: Session Id: $ cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cvpdnNotifSessionEvent	Indicates the event that generated the L2X session notification. The events are represented as follows: up: Session has come up. down: Session has gone down. pwUp: Pseudowire associated with this session has come up. pwDown: Pseudowire associated with this session has gone down. INTEGER is unknown
cvpdnNotifSessionID	This object contains the local session ID of the L2X session for which this notification has been generated.
cvpdnSessionAttrDevicePhyId	The device ID of the physical interface for the session. The object is the the interface index which points to the ifTable. For virtual interfaces that are not in the ifTable, the value will be zero.
cvpdnSessionAttrVirtualCircuitID	The virtual circuit ID of an active Layer 2 VPN session.
cvpdnSystemTunnelType	The tunnel type. This is the tunnel protocol.
cvpdnTunnelAttrTunnelId	The Tunnel ID of an active VPDN tunnel. If this end is the instigator of the tunnel, the ID is the TS tunnel ID, otherwise it is the NAS tunnel ID. Two distinct tunnels with the same tunnel ID may exist, but with different tunnel types.
cvpdnSessionAttrSessionId	The ID of an active VPDN session.

Go Top

SECTION 11.15

Trap: cvpdnNotifSession

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
VPDNSessionPseudowireState	Trap	Event	No	Normal	$NodeDisplayName - The VPDN session pseudowire is up: Session Id: $cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID	VPDNSessionPseudowireState	PDSN
VPDNSessionPseudowireState	Trap	Event	No	Warning	$NodeDisplayName - The VPDN session pseudowire is down: Session Id: $cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID.	VPDNSessionPseudowireState	PDSN

Description:

```
Conveys an event regarding the L2X session with the indicated session ID and Xconnect VCID.
```

Default Message:

$NodeDisplayName - The VPDN session is down: Session Id: $ cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID
$NodeDisplayName - The VPDN session is up: Session Id: $ cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID
$NodeDisplayName - The VPDN session pseudowire is down: Session Id: $ cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID
$NodeDisplayName - The VPDN session pseudowire is up: Session Id: $ cvpdnNotifSessionID, Device Id: $cvpdnSessionAttrDevicePhyId, Virtual Circuit Id: $cvpdnSessionAttrVirtualCircuitID

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cvpdnNotifSessionEvent	Indicates the event that generated the L2X session notification. The events are represented as follows: up: Session has come up. down: Session has gone down. pwUp: Pseudowire associated with this session has come up. pwDown: Pseudowire associated with this session has gone down. INTEGER is unknown
cvpdnNotifSessionID	This object contains the local session ID of the L2X session for which this notification has been generated.
cvpdnSessionAttrDevicePhyId	The device ID of the physical interface for the session. The object is the the interface index which points to the ifTable. For virtual interfaces that are not in the ifTable, the value will be zero.
cvpdnSessionAttrVirtualCircuitID	The virtual circuit ID of an active Layer 2 VPN session.
cvpdnSystemTunnelType	The tunnel type. This is the tunnel protocol.
cvpdnTunnelAttrTunnelId	The Tunnel ID of an active VPDN tunnel. If this end is the instigator of the tunnel, the ID is the TS tunnel ID, otherwise it is the NAS tunnel ID. Two distinct tunnels with the same tunnel ID may exist, but with different tunnel types.
cvpdnSessionAttrSessionId	The ID of an active VPDN session.

Go Top

SECTION 12.1

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigModified	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was modified.	APN-ConfigModified	SGW

Description:

```
A notification of this type is generated when an              entry is generated in the
cgprsAccPtCfgNotifHistTable and
cgprsAccPtCfgNotifEnable is set to true.
```

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 12.2

Trap: cgprsAccPtSecSrcViolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-UpstreamSecurityViolation	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- Upstream security violation.	APN-UpstreamSecurityViolation	SGW

Description:

A notification of this type is generated when security violation as specified by cgprsAccPtVerifyUpStrTpduSrcAddr occurs on an APN.

Default Message:

$NodeDisplayName -- APN ($cgprsAccPtCfgNotifAccPtIndex) Upstream security violation.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtMsAddrType	This object specifies the type of Internet address denoted by cgprsAccPtMsAllocAddr, cgprsAccPtMsNewAddr and cgprsAccPtMsTpduDstAddr.
cgprsAccPtMsAllocAddr	This object specifies the IP address that is assigned to the MS during PDP activation.
cgprsAccPtMsNewAddr	This object specifies the fake IP address that is used by the MS.

Go Top

SECTION 12.3

Trap: cgprsAccPtSecDestViolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-DownstreamSecurityViolation	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- Downstream security violation.	APN-DownstreamSecurityViolation	SGW

Description:

```
A notification of this type is generated when security violation as specified by
cgprsAccPtVerifyUpStrTpduDstAddr occurs on an APN.
```

Default Message:

$NodeDisplayName -- APN ($cgprsAccPtCfgNotifAccPtIndex) Downstream security violation.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtMsAddrType	This object specifies the type of Internet address denoted by cgprsAccPtMsAllocAddr, cgprsAccPtMsNewAddr and cgprsAccPtMsTpduDstAddr.
cgprsAccPtMsAllocAddr	This object specifies the IP address that is assigned to the MS during PDP activation.
cgprsAccPtMsTpduDstAddr	This object specifies the upstream TPDU destination address used by a MS that falls in the reserved range of IP addresses for PLMN devices.

Go Top

SECTION 12.4

Trap: cgprsAccPtMaintenanceNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ServiceMode	Trap	Alarm	Yes	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in maintenance mode.	APN-ServiceMode	SGW
APN-ServiceMode	Trap	Alarm	Yes	Normal	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in service.	APN-ServiceMode	SGW
APN-ServiceMode	Poll	Alarm	Yes	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in maintenance mode.	APN-ServiceMode	SGW
APN-ServiceMode	Poll	Alarm	Yes	Normal	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in service.	APN-ServiceMode	SGW

Description:

```
A notification of this type is generated when APN is placed in maintenance mode which is specified by
cgprsAccPtOperationMode.
```

Default Message:

$NodeDisplayName -- The APN ($cgprsAccPtCfgNotifAccPtIndex) is in maintenance mode.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.

Go Top

SECTION 12.5

Trap: cgprsCgInServiceModeNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	SGW
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	SGW
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	SGW
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	SGW
ChargingGatewayMaintenanceMode	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	SGW
ChargingGatewayMaintenanceMode	Poll	Alarm	Yes	Warning	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	SGW

Description:

```
A notification of this type is generated when the        gateway charging function is in normal mode. This can
be identified by cgprsCgServiceMode object.
```

Default Message:

$NodeDisplayName -- The charging gateway is in service.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 12.6

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is down.	ChargingGatewayState	SGW
ChargingGatewayState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is up.	ChargingGatewayState	SGW
ChargingGatewayState	Trap	Alarm	Yes	Critical	$NodeDisplayName - The Charging gateway is down	ChargingGatewayState	SGW
ChargingGatewayState	Trap	Alarm	Yes	Normal	$NodeDisplayName - The Charging gateway is up	ChargingGatewayState	SGW

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.

$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 12.7

Trap: cgprsCgGatewaySwitchoverNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewaySwitchover	Trap	Alarm	No	Major	$NodeDisplayName -- The charging gateway switched from $cgprsCgOldChgGatewayAddress to $cgprsCgActiveChgGatewayAddress	ChargingGatewaySwitchover	SGW
ChargingGatewaySwitchover	Trap	Alarm	No	Major	$NodeDisplayName -- The charging gateway switched from $cgprsCgGatewayGroupStatusOldCgAddr to $cgprsCgGatewayGroupStatusActiveCgAddr	ChargingGatewaySwitchover	SGW

Description:

A notification of this type is generated when the charging gateway is switched, the new charging gateway is identified by cgprsCgActiveChgGatewayAddress and the old charging gateway is identified by cgprsCgOldChgGatewayAddress.
The switchover will happen according to the value set in cgprsCgGroupSwitchOverTime and the selection of the new CG will be according to the value set in cgprsCgSwitchOverPriority.

Default Message:

$NodeDisplayName -- The charging gateway switched from $cgprsCgOldChgGatewayAddress to $cgprsCgActiveChgGatewayAddress

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgActiveChgGatewayAddrType	This object specifies the address type of the active charging gateway.

cgprsCgActiveChgGatewayAddress	This object specifies the address of the active charging gateway. The type of address will be represented by cgprsCgActiveChgGatewayAddrType.
cgprsCgOldChgGatewayAddress	This object specifies the address of the previous active charging gateway. The type of address will same as the one present in cgprsCgActiveChgGatewayAddrType.

Go Top

SECTION 12.8

Trap: cGtpPathFailedNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPPathFailed	Trap	Alarm	No	Major	$NodeDisplayName -- Peer ($cGtpLastNoRespToEchoGSNIpAddr) failed to respond to the GTP Echo Request.	GTPPathFailed	SGW

Description:

This notification is sent when one of this GSN's peers failed to respond to the GTP 'Echo Request' message for the waiting interval.

Default Message:

$NodeDisplayName -- Peer ($cGtpLastNoRespToEchoGSNIpAddr) failed to respond to the GTP Echo Request.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGtpLastNoRespToEchoGSNIpAddrTyp	This object indicates the type of Internet address by which cGtpLastNoRespToEchoGSNIpAddr is reachable.
cGtpLastNoRespToEchoGSNIpAddr	The IP address of the last peer GSN device that did not reply to an GTP 'Echo Request' message from the local GSN device.

Go Top

SECTION 12.9

Trap: cGgsnSADccaRatingFailed

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCARatingFail	Trap	Alarm	No	Major	$NodeDisplayName -- The Credit Control Server cannot rate a service request for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCARatingFail	SGW

Description:

This notification is generated when the credit-control server cannot rate the service request, due to insufficient rating input, incorrect AVP combination or due to an AVP or an AVP value that is not recognized or supported in the rating.

Default Message:

$NodeDisplayName -- The Credit Control Server cannot rate a service request for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 12.10

Trap: cGgsnSADccaEndUsrServDeniedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCAServiceDenied	Trap	Alarm	No	Major	$NodeDisplayName -- The Credit Control Server denied a service request due to service restrictions for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCAServiceDenied	SGW

Description:

This notification is generated when the credit-control server denies the service request due to service restrictions. On reception of this notif on category level, the CLCI-C shall discard all future user traffic for that category on that PDP context and not attempt to ask for more quotas during the same PDP context.

Default Message:

$NodeDisplayName -- The Credit Control Server denied a service request due to service restrictions for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 12.11

Trap: cGgsnSACsgStateDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CSGState	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The CSG is down.	CSGState	SGW
CSGState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The CSG is up.	CSGState	SGW

Description:

```
This notification is generated when CSG state goes         down.
```

Default Message:

$NodeDisplayName -- The CSG is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnSANotifCsgRealAddressType	This object indicates the type of IP address, for real address of the CSG group.
cGgsnSANotifCsgRealAddress	This object indicates the real IP address of the CSG group.
cGgsnSANotifCsgVirtualAddrType	This object indicates the type of IP address, for virtual address of the CSG group.
cGgsnSANotifCsgVirtualAddress	This object indicates the virtual IP address of the CSG group.
cGgsnSANotifCsgPort	This object indicates the port number of the CSG group.

Go Top

SECTION 12.12

Trap: cGgsnSADccaCreditLimReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCACreditLimitReached	Trap	Alarm	No	Major	$NodeDisplayName -- Credit limit reached for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCACreditLimitReached	SGW

Description:

```
This notification is generated when the credit limit          is reached.  The credit-control server denies the service
request since the end user's account could not cover the
requested service.  Client shall behave exactly as with
cGgsnSADccaEndUsrServDeniedNotif.
```

Default Message:

$NodeDisplayName -- Credit limit reached for $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 12.13

Trap: cGgsnSADccaUserUnknownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCAUserUnknown	Trap	Alarm	No	Major	$NodeDisplayName -- User is unknown in the Credit Control Server $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn	DCCAUserUnknown	SGW

Description:

This notification is generated when the specified end user is unknown in the credit-control server. Such permanent failures cause the client to enter the Idle state. The client shall reject or terminate the PDP context depending on whether the result code was received in a CCA (Initial) or CCA (Update).

Default Message:

$NodeDisplayName -- User is unknown in the Credit Control Server $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 12.14

Trap: cGgsnSADccaAuthRejectedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DCCAAuthReject	Trap	Alarm	No	Major	$NodeDisplayName -- The Credit Control Server rejected authorization of user $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn.	DCCAAuthReject	SGW

Description:

```
This notification is generated when credit-control          server failed in authorization of end user.  The PDP
context is deleted and category is blacklisted.
```

Default Message:

$NodeDisplayName -- The Credit Control Server rejected authorization of user $cGgsnNotifPdpImsi / $cGgsnNotifPdpMsisdn.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

Go Top

SECTION 12.15

Trap: cGgsnGlobalErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWServiceState	Trap	Alarm	Yes	Critical	$NodeDisplayName -- The gateway service is shutdown. Reason: $cGgsnHistNotifInfo	GWServiceState	SGW
GWServiceState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway service is started. Reason: $cGgsnHistNotifInfo	GWServiceState	SGW

Description:

```
This notification indicates the occurrence of a gateway        related alarm.
```

Default Message:

$NodeDisplayName -- The gateway service is shutdown.
$NodeDisplayName -- The gateway service is started.
$NodeDisplayName -- MAP-SGSN service is shutdown.
$NodeDisplayName -- MAP-SGSN service is started.
$NodeDisplayName -- No DHCP server is configured.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnGlobalErrorTypes	This object indicates the types of global errors as follows. 'ggsnServiceUp' - Gateway service has started 'ggsnServiceDown' - Gateway service is shutdown 'mapSgsnUp' - MAP-SGSN service has started 'mapSgsnDown' - MAP-SGSN service is shutdown 'noDHCPServer' -- DHCP server is not configured

cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

Go Top

SECTION 12.16

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-NoResources	Trap	Alarm	No	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached. Reason: $cGgsnHistNotifInfo	APN-NoResources	SGW

Description:

This notification indicates the occurrence of a User related alarm.

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).

cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 12.17

Trap: cGgsnMaintenanceNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is in maintenance mode.	GWMaintenanceMode	SGW
GWMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is in service.	GWMaintenanceMode	SGW
GWMaintenanceMode	Poll	Alarm	Yes	Major	$NodeDisplayName -- The gateway is in maintenance mode.	GWMaintenanceMode	SGW
GWMaintenanceMode	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is in service.	GWMaintenanceMode	SGW

Description:

A notification of this type is generated when the gateway is placed in maintenance mode which is specified by cGgsnServiceModeStatus.

Default Message:

$NodeDisplayName -- The gateway is in maintenance mode.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 12.18

Trap: cGgsnAccessPointNameNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-NoRadius	Trap	Alarm	No	Major	APN $ApnDisplayName on the gateway $NodeDisplayName -- No RADIUS server is configured. $cGgsnHistNotifInfo	APN-NoRadius	SGW

Description:

```
This notification indicates the occurrence of a APN       related alarm.
```

Default Message:

$NodeDisplayName -- No RADIUS server is configured. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- IP address allocation failed. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- Access point is not reachable. ($cGgsnNotifAccessPointName)

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnAccessPointErrorTypes	This object indicates the types access point errors as follows. 'noRadius' - RADIUS Server is not configured. 'ipAllocationFail' - Unable to allocate IP address. 'apnUnreachable' - Unable to reach access point.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 12.19

Trap: cGgsnMemThresholdClearedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWMemoryThreshold	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway memory threshold is cleared. The gateway memory overload protection mechanism is disengaged.	GWMemoryThreshold	SGW
					$NodeDisplayName -- The gateway memory threshold is reached. The gateway memory overload		

GWMemoryThreshold	Trap	Alarm	Yes	Critical	protection mechanism is engaged.	GWMemoryThreshold	SGW

Description:

```
A notification of this type is generated when the gateway       retains the memory and falls below threshold value
speficied by cGgsnMemoryThreshold.
```

Default Message:

$NodeDisplayName -- The gateway memory threshold is cleared. The gateway memory overload protection mechanism is disengaged

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 12.20

Trap: cGgsnAccessPointNameNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-IpAllocationFail	Trap	Alarm	No	Critical	APN $ApnDisplayName on the gateway $NodeDisplayName -- IP address allocation failed. $cGgsnHistNotifInfo	APN-IpAllocationFail	SGW

Description:

```
This notification indicates the occurrence of a APN       related alarm.
```

Default Message:

$NodeDisplayName -- No RADIUS server is configured. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- IP address allocation failed. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- Access point is not reachable. ($cGgsnNotifAccessPointName)

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnAccessPointErrorTypes	This object indicates the types access point errors as follows. 'noRadius' - RADIUS Server is not configured. 'ipAllocationFail' - Unable to allocate IP address. 'apnUnreachable' - Unable to reach access point.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.

cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 12.21

Trap: cGgsnAccessPointNameNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-Unreachable	Trap	Alarm	No	Critical	APN $ApnDisplayName on the gateway $NodeDisplayName -- Access point is not reachable. $cGgsnHistNotifInfo	APN-Unreachable	SGW

Description:

This notification indicates the occurrence of a APN related alarm.

Default Message:

$NodeDisplayName -- No RADIUS server is configured. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- IP address allocation failed. ($cGgsnNotifAccessPointName)
$NodeDisplayName -- Access point is not reachable. ($cGgsnNotifAccessPointName)

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnAccessPointErrorTypes	This object indicates the types access point errors as follows. 'noRadius' - RADIUS Server is not configured. 'ipAllocationFail' - Unable to allocate IP address. 'apnUnreachable' - Unable to reach access point.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 12.22

Trap: cGgsnGlobalErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
MapSgsnState	Trap	Alarm	Yes	Major	$NodeDisplayName -- MAP-SGSN service is shutdown. Reason: $cGgsnHistNotifInfo	MapSgsnState	SGW
MapSgsnState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- MAP-SGSN service is started. Reason: $cGgsnHistNotifInfo	MapSgsnState	SGW

Description:

This notification indicates the occurrence of a gateway related alarm.

Default Message:

$NodeDisplayName -- The gateway service is shutdown.
$NodeDisplayName -- The gateway service is started.
$NodeDisplayName -- MAP-SGSN service is shutdown.
$NodeDisplayName -- MAP-SGSN service is started.
$NodeDisplayName -- No DHCP server is configured.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnGlobalErrorTypes	This object indicates the types of global errors as follows. 'ggsnServiceUp' - Gateway service has started 'ggsnServiceDown' - Gateway service is shutdown 'mapSgsnUp' - MAP-SGSN service has started 'mapSgsnDown' - MAP-SGSN service is shutdown 'noDHCPServer' -- DHCP server is not configured
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

Go Top

SECTION 12.23

Trap: cGgsnGlobalErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NoDHCPServer	Trap	Alarm	No	Major	$NodeDisplayName -- No DHCP server is configured. Reason: $cGgsnHistNotifInfo	NoDHCPServer	SGW

Description:

```
This notification indicates the occurrence of a gateway        related alarm.
```

Default Message:

$NodeDisplayName -- The gateway service is shutdown.
$NodeDisplayName -- The gateway service is started.
$NodeDisplayName -- MAP-SGSN service is shutdown.
$NodeDisplayName -- MAP-SGSN service is started.
$NodeDisplayName -- No DHCP server is configured.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnGlobalErrorTypes	This object indicates the types of global errors as follows. 'ggsnServiceUp' - Gateway service has started 'ggsnServiceDown' - Gateway service is shutdown 'mapSgsnUp' - MAP-SGSN service has started 'mapSgsnDown' - MAP-SGSN service is shutdown 'noDHCPServer' -- DHCP server is not configured
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

Go Top

SECTION 12.24

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-AuthenticationFail	Trap	Alarm	No	Minor	APN $ApnDisplayName on gateway $NodeDisplayName -- A PDP activation failed because of an authentication failure. Reason: $cGgsnHistNotifInfo	APN-AuthenticationFail	SGW

Description:

```
This notification indicates the occurrence of a User        related alarm.
```

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-CCRInitFail	Trap	Alarm	No	Minor	APN $ApnDisplayName on gateway $NodeDisplayName -- The TX timer expired before getting a CCR (initial) response. Reason: $cGgsnHistNotifInfo	APN-CCRInitFail	SGW

Description:

```
This notification indicates the occurrence of a User        related alarm.
```

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.
cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.

cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 12.26

Trap: cGgsnPacketDataProtocolNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-QuotaPushFail	Trap	Alarm	No	Minor	APN $ApnDisplayName on gateway $NodeDisplayName -- Quota Push failed to the CSG quota server. Reason: $cGgsnHistNotifInfo	APN-QuotaPushFail	SGW

Description:

This notification indicates the occurrence of a User related alarm.

Default Message:

$NodeDisplayName -- A PDP activation failed because of an authentication failure.
$NodeDisplayName -- The TX timer expired before getting a CCR (initial) response.
$NodeDisplayName -- Quota Push failed to the CSG quota server.
$NodeDisplayName -- Resources to continue the gateway service have been exhausted because the maximum number of PDP contexts has been reached.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnPacketDataProtoErrorTypes	This object indicates the types of Packet Data Protocol errors as follows. 'noResource' - Mobile Station initiated PDP count reaches the specified limit or Network initiated PDP count reaches the specified limit. 'authenticationFail' - Authentication failed. 'ccrInitFail' - CCR(initial)is sent to diameter server, and Tx timer expires before getting CCA (initial) response. The action on the PDP context creation is determined by the configured failure handling, as specified in cGgsnSADccaCcfh object in CISCO-GGSN-SERVICE-AWARE-MIB. 'quotaPushFail' - Quota Push failed, when the path between CSG-QS is down or when CSG sends a negative Response for quota push request.
cGgsnHistNotifSeverity	This object indicates the severity level of the notification. This object cannot be set to cleared(1) or indeterminate(2).
cGgsnHistNotifTimestamp	This object indicates the value of sysUpTime when this notification was generated.
cGgsnHistNotifGgsnIpAddrType	This object indicates the type of Internet address by which cGgsnHistNotifGgsnIpAddr is reachable.
cGgsnHistNotifGgsnIpAddr	The object indicates the IP address that uniquely identifies the device which generated the notification.
cGgsnHistNotifInfo	A textual description of cGgsnHistNotifType, which potentially contains additional information (more than just the type of alarm). If the text of the message exceeds 64 bytes, the message will be truncated to 63 bytes and a '*' character will be appended to indicate the message has been truncated.

cGgsnNotifPdpImsi	This object specifies the International Mobile Subscriber Identity (IMSI) of the user for whom the notification is generated. This object is used to specify IMSI of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifPdpMsisdn	This object specifies the Mobile Subscriber ISDN (MSISDN) value of the user for whom the notification is generated. This object is used to specify MSISDN of the user in the cGgsnPacketDataProtocolNotif notification.
cGgsnNotifAccessPointName	This object specifies the Access Point Name and is used specify the name in the cGgsnAccessPointNameNotif notification.

Go Top

SECTION 12.27

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigCreated	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was created.	APN-ConfigCreated	SGW

Description:

A notification of this type is generated when an entry is generated in the cgprsAccPtCfgNotifHistTable and cgprsAccPtCfgNotifEnable is set to true.

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 12.28

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigDeleted	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was deleted.	APN-ConfigDeleted	SGW

Description:

A notification of this type is generated when an entry is generated in the cgprsAccPtCfgNotifHistTable and cgprsAccPtCfgNotifEnable is set to true.

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 12.29

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingTransferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.	ChargingTransferState	SGW
ChargingTransferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.	ChargingTransferState	SGW
ChargingTransferState	Trap	Alarm	Yes	Major	$NodeDisplayName - The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway	ChargingTransferState	SGW
ChargingTransferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.	ChargingTransferState	SGW

Description:

A cgprsCgAlarmNotif signifies that a GPRS related alarm is detected in the managed system. This alarm is sent after an entry has been added to cgprsCgAlarmHistTable.

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 12.30

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingCapacityState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.	ChargingCapacityState	SGW
ChargingCapacityState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.	ChargingCapacityState	SGW
ChargingCapacityState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.	ChargingCapacityState	SGW
ChargingCapacityState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs	ChargingCapacityState	SGW

Description:

A cgprsCgAlarmNotif signifies that a GPRS related alarm is detected in the managed system. This alarm is sent after an entry has been added to cgprsCgAlarmHistTable.

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.

cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 12.31

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayEchoState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.	ChargingGatewayEchoState	SGW
ChargingGatewayEchoState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway received an echo response from the charging gateway.	ChargingGatewayEchoState	SGW
ChargingGatewayEchoState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.	ChargingGatewayEchoState	SGW
ChargingGatewayEchoState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway received an echo response from the charging gateway.	ChargingGatewayEchoState	SGW

Description:

A cgprsCgAlarmNotif signifies that a GPRS related alarm is detected in the managed system. This alarm is sent after an entry has been added to cgprsCgAlarmHistTable.

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.

cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 12.32

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingCDRBufferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has discarded G-CDRs.	ChargingCDRBufferState	SGW
ChargingCDRBufferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.	ChargingCDRBufferState	SGW
ChargingCDRBufferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has discarded G-CDRs.	ChargingCDRBufferState	SGW
ChargingCDRBufferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.	ChargingCDRBufferState	SGW

Description:

A cgprsCgAlarmNotif signifies that a GPRS related alarm is detected in the managed system. This alarm is sent after an entry has been added to cgprsCgAlarmHistTable.

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	Type of the GPRS charging gateway or charging related alarm.
cgprsCgAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.
cgprsCgAlarmHistAddress	The IP address that is used to uniquely identify the CG.
cgprsCgAlarmHistSeverity	This object indicates the severity of the alarm.
cgprsCgAlarmHistInfo	This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.

Go Top

SECTION 12.33

Trap: cgprsCgAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging transactions on the gateway are disabled.	ChargingState	SGW
ChargingState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging transactions on the gateway are enabled.	ChargingState	SGW
ChargingState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging transactions on the gateway are disabled.	ChargingState	SGW
ChargingState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging transactions on the gateway are enabled	ChargingState	SGW

Description:

```
A cgprsCgAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgAlarmHistTable.
```

Default Message:

$NodeDisplayName -- The charging gateway is down.
$NodeDisplayName -- The charging gateway is up.
$NodeDisplayName -- The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway after the failure.
$NodeDisplayName -- The gateway is out of memeory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- the gateway received the echo response from the charging gateway after the echo failure has been detected.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgAlarmHistType	`Type of the GPRS charging gateway or charging related alarm.`
cgprsCgAlarmHistAddrType	`This object indicates the type of Internet address given in cgprsCgAlarmHistAddress.`
cgprsCgAlarmHistAddress	`The IP address that is used to uniquely identify the CG.`
cgprsCgAlarmHistSeverity	`This object indicates the severity of the alarm.`
cgprsCgAlarmHistInfo	`This object provide detailed information when a GPRS charging gateway or charging related alarm is generated.`

Go Top

SECTION 12.34

Trap: ciscoDiaBaseProtPeerConnectionDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPeerConnectionState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	SGW

DiameterPeerConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	SGW
DiameterPeerConnectionState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	SGW
DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	SGW
DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	SGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitConnAck.	DiameterPeerConnectionState	SGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitICEA.	DiameterPeerConnectionState	SGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is elect.	DiameterPeerConnectionState	SGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitReturns.	DiameterPeerConnectionState	SGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is closing.	DiameterPeerConnectionState	SGW

Description:

```
An ciscoDiaBaseProtPeerConnectionDownNotif notification           is sent when both the following conditions are true:
1) the value of
ciscoDiaBaseProtEnablePeerConnectionDownNotif is true(1)
2) cdbpPeerStatsState changes to closed(1).
It can be utilized by an NMS to trigger logical/physical
entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The peer $cdbpPeerId state is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpLocalId	The implementation identification string for the Diameter software in use on the system, for example; 'diameterd'
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 12.35

Trap: ciscoDiaBaseProtPermanentFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPermanentFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol permanent failures for the diameter peer $cdbpPeerId has increased.	DiameterPermanentFailure	SGW

Description:

```
An ciscoDiaBaseProtPermanentFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnablePermanentFailureNotif
   is true(1)
2) the value of cdbpPeerStatsPermanentFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol permanent failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsPermanentFailures	This object represents the Number of permanent failures returned to peer.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 12.36

Trap: ciscoDiaBaseProtProtocolErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterProtocolError	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol errors returned to the diameter peer $cdbpPeerId has increased.	DiameterProtocolError	SGW

Description:

```
An ciscoDiaBaseProtProtocolErrorNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableProtocolErrorNotif
   is true(1)
2) the value of cdbpPeerStatsProtocolErrors changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol errors returned to the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsProtocolErrors	This object represents the Number of protocol errors returned to peer, but not including redirects.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 12.37

Trap: ciscoDiaBaseProtTransientFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterTransientFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol transient failures for the diameter peer $cdbpPeerId has increased.	DiameterTransientFailure	SGW

Description:

```
An ciscoDiaBaseProtTransientFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableTransientFailureNotif
   is true(1)
2) the value of cdbpPeerStatsTransientFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol transient failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsTransientFailures	This object represents the transient failure count.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 12.38

Trap: cegCongestionClearedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-GW-CongestionState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus.	EPC-GW-CongestionState	SGW
EPC-GW-CongestionState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus. This gateway is rejecting all new calls.	EPC-GW-CongestionState	SGW
EPC-GW-CongestionState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus. This gateway is rejecting low priority calls.	EPC-GW-CongestionState	SGW
EPC-GW-CongestionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The EPC Gateway congestion status is normal.	EPC-GW-CongestionState	SGW
EPC-GW-CongestionState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The EPC Gateway congestion status is high. This gateway is rejecting all new calls.	EPC-GW-CongestionState	SGW
EPC-GW-CongestionState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- The EPC Gateway congestion status is low. This gateway is rejecting low priority calls.	EPC-GW-CongestionState	SGW

Description:

```
The gateway sends this notification, when       the gateway congestion level goes below
cegLowCongestionThreshold value.
This gives an indication that the gateway
has recovered from congestion and it can
accept all calls.
```

Default Message:

$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegVersion	This object represents the current version of the PGW or SGW software running on the gateway. Display format: : :.
cegCongestionStatus	This object represents the gateway congestion status. INTEGER is unknown
cegCongestionDfpWeight	This object represents the dfp value, which is used to measure the congestion level in the gateway.
cegCongestionLowThreshold	This object represents the low threshold for congestion. Congestion DFP metric considers the current CPU memory usage and number of bearers open. On reaching the low congestion threshold, based on the ARP, high priority calls are accepted and those with a lower priority are rejected. When the gateway congestion level goes below this value, the gateway send cegCongestionClearedNotif notification. This notification would indicate that the gateway has recovered from congestion.

Go Top

SECTION 12.39

Trap: cegqCacMaxPdpExceededNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-MaxPdpExceeded	Trap	Alarm	No	Major	$NodeDisplayName -- The number of pdps on the gateway has reached the user-configured maximum of $cegqCacMaxPdpContext for the CAC policy $cegqCacMaxPdpContext_cegqCacPolicyName.	EPC-QOS-MaxPdpExceeded	SGW

Description:

```
This notification is sent when the number of pdps on the       gateway has reached the user-configured maximum (or threshold).
```

Default Message:

$NodeDisplayName -- The number of pdps on the gateway has reached the user-configured maximum of $cegqCacMaxPdpContext for the CAC policy $cegqCacMaxPdpContext_cegqCacPolicyName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqCacMaxPdpContext	This object defines maximum number that can be created. If total number of activated pdp exceeds the maximum number, the pdp request will be rejected. Value '0' means there is no limit on pdp creation.
cegqCacPolicyName	This object is the CAC policy name which will be attached to one or more APN's.

Go Top

SECTION 12.40

Trap: cegqCacUpgBRateBearerRejNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-BearerRejected	Trap	Alarm	No	Major	$NodeDisplayName -- The gateway is rejecting bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate	EPC-QOS-BearerRejected	SGW

Description:

```
This notification is sent when bearers are Rejected/Downgraded       by CAC due to requesting for higher bit rate than
user-configured maximum for a certain QCI class.
```

Default Message:

$NodeDisplayName -- The gateway is rejecting bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqCacQciReject	This object is to specify whether the requested MBR/GBR be downgraded or bearer to be rejected if the requested MBR/GBR exceeds the value set in cegqCacQciBitRateType. 'true' - The request will be rejected if exceeded. 'false' - The requested MBR will be downgraded if exceeded. Represents a boolean value.
cegqCacQciBitRate	This object specifies the MBR/GBR allowed for the QCI defined by cegqCacQci.
cegqCacQci	This object specifies the QCI for which MBR/GBR in uplink/downlink has to be set. When the ratetype is set to guaranteed,QCI1-QCI4 are allowed. When the ratetype is set to maximum,QCI1-QCI9 are allowed.
cegqCacQciBitRateType	This object specifies the type of bit rate applicable for QCI denoted by cegqCacQci.
cegqCacQciDirection	This object specifies the direction of traffic.
cegqCacPolicyName	This object is the CAC policy name which will be attached to one or more APN's.

Go Top

SECTION 12.41

Trap: cegqCacUpgBRateBearerRejNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-BearerDowngraded	Trap	Alarm	No	Minor	$NodeDisplayName -- The gateway is downgrading bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate	EPC-QOS-BearerDowngraded	SGW

Description:

```
This notification is sent when bearers are Rejected/Downgraded       by CAC due to requesting for higher bit rate than
user-configured maximum for a certain QCI class.
```

Default Message:

$NodeDisplayName -- The gateway is rejecting bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqCacQciReject	This object is to specify whether the requested MBR/GBR be downgraded or bearer to be rejected if the requested MBR/GBR exceeds the value set in cegqCacQciBitRateType. 'true' - The request will be rejected if exceeded. 'false' - The requested MBR will be downgraded if exceeded. Represents a boolean value.
cegqCacQciBitRate	This object specifies the MBR/GBR allowed for the QCI defined by cegqCacQci.
cegqCacQci	This object specifies the QCI for which MBR/GBR in uplink/downlink has to be set. When the ratetype is set to guaranteed,QCI1-QCI4 are allowed. When the ratetype is set to maximum,QCI1-QCI9 are allowed.
cegqCacQciBitRateType	This object specifies the type of bit rate applicable for QCI denoted by cegqCacQci.
cegqCacQciDirection	This object specifies the direction of traffic.
cegqCacPolicyName	This object is the CAC policy name which will be attached to one or more APN's.

Go Top

SECTION 12.42

Trap: cegqQciBWMaxReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-MaxBandwidthReached	Trap	Alarm	No	Warning	$NodeDisplayName -- The bandwidth available is fully utilized. No more bearers can be admitted for this QCI class.	EPC-QOS-MaxBandwidthReached	SGW

Description:

```
This notification is sent when the bandwidth allocated for a       certain QCI class has been fully utilized and no further bearer
can be admitted for this QCI class. The notification is sent
when the bandwidth pool utilization reaches the value in
the object cegqBWPoolQciAbsVal.
```

Default Message:

$NodeDisplayName -- The bandwidth available is fully utilized. No more bearers can be admitted for this QCI class.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router

	that sent the trap.
cegqBWPoolQciAbsVal	This object denotes the absolute value of bandwidth allocated for the QCI set in cegqBWPoolQci.
cegqBWPoolQciAvailBw	This object denotes the absolute available bandwidth left unused for QCI set in cegqBWPoolQci.
cegqBWPoolQci	This object defines the QCI for which the allocation of bandwidth is needed.
cegqCacBWPoolName	This object is the name of the virtual bandwidth pool which will be attached to the APN.

Go Top

SECTION 12.43

Trap: cIscsiInstSessionFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-InstanceSessionState	Trap	Alarm	No	Warning	$NodeDisplayName - The active session has failed for the remote node - $cIscsiInstLastSsnRmtNodeName.	iSCSI-InstanceSessionState	SGW

Description:

```
Sent when an active session is failed by either the initiator        or the target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The active session has failed for the remote node $cIscsiInstLastSsnRmtNodeName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiInstSsnFailures	This object counts the number of times a session belonging to this instance has been failed.
cIscsiInstLastSsnFailureType	The counter object in the cIscsiInstSsnErrorStatsTable that was incremented when the last session failure occurred. If the reason for failure is not found in the cIscsiInstSsnErrorStatsTable, the value { 0.0 } is used instead.
cIscsiInstLastSsnRmtNodeName	An octet string describing the name of the remote node from the failed session.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.

Go Top

SECTION 12.44

Trap: cIscsiIntrLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-InitiatorLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.	iSCSI-InitiatorLoginStatus	SGW

Description:

```
Sent when a login is failed by a initiator.
```

```
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiIntrLastTgtFailureAddrType	The type of Internet Network Address in cIscsiIntrLastTgtFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiIntrLoginFailures	This object counts the number of times a login attempt from this local initiator has failed.
cIscsiIntrLastFailureType	The type of the most recent failure of a login attempt from this initiator, represented as the OID of the counter object in cIscsiInitiatorLoginStatsTable for which the relevant instance was incremented. A value of 0.0 indicates a type which is not represented by any of the counters in cIscsiInitiatorLoginStatsTable.
cIscsiIntrLastTgtFailureName	An octet string giving the name of the target that failed the last login attempt.
cIscsiIntrLastTgtFailureAddr	An Internet Network Address giving the host address of the target that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular

	ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

SECTION 12.45

Trap: cIscsiTgtLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-TargetLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.	iSCSI-TargetLoginStatus	SGW

Description:

```
Sent when a login is failed by a target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiTgtLastIntrFailureAddrType	The type of Internet Network Address in cIscsiTgtLastIntrFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation.

	Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiTgtLoginFailures	This object counts the number of times a login attempt to this local target has failed.
cIscsiTgtLastFailureType	The type of the most recent failure of a login attempt to this target, represented as the OID of the counter object in cIscsiTargetLoginStatsTable for which the relevant instance was incremented. A value of 0.0 indicates a type which is not represented by any of the counters in cIscsiTargetLoginStatsTable.
cIscsiTgtLastIntrFailureName	An octet string giving the name of the initiator that failed the last login attempt.
cIscsiTgtLastIntrFailureAddr	An Internet Network Address giving the host address of the initiator that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

SECTION 12.46

Trap: ciscoTap2MediationTimedOut

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationTimedOut	Trap	Alarm	Yes	Normal	$NodeDisplayName - Tap2Mediation status is active.	Tap2MediationTimedOut	SGW
Tap2MediationTimedOut	Trap	Alarm	Yes	Critical	$NodeDisplayName - Tap2Mediation status is notInService.	Tap2MediationTimedOut	SGW
Tap2MediationTimedOut	Trap	Alarm	Yes	Warning	$NodeDisplayName - Tap2Mediation status is notReady.	Tap2MediationTimedOut	SGW
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndGo.	Tap2MediationTimedOut	SGW
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndWait.	Tap2MediationTimedOut	SGW
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is destroy.	Tap2MediationTimedOut	SGW

Description:

```
When an intercept is autonomously removed by an intercepting       device, such as due to the time specified in
cTap2MediationTimeout arriving, the device notifies the manager
of the action.
```

Default Message:

$NodeDisplayName - Tap2Mediation status is active.
$NodeDisplayName - Tap2Mediation status is notReady.
$NodeDisplayName - Tap2Mediation status is notInService.
$NodeDisplayName - Tap2Mediation status is createAndGo.
$NodeDisplayName - Tap2Mediation status is createAndWait.
$NodeDisplayName - Tap2Mediation status is destroy.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2MediationStatus	The status of this conceptual row. This object is used to manage creation, modification and deletion of rows in this

table.
cTap2MediationTimeout may be modified at any time (even while the row is active). But when the row is active, the other writable objects may not be modified without setting its value to 'notInService'.
The entry may not be deleted or deactivated by setting its value to 'destroy' or 'notInService' if there is any associated entry in cTap2StreamTable.
The RowStatus textual convention is used to manage the creation and deletion of conceptual rows, and is used as the value of the SYNTAX clause for the status column of a conceptual row (as described in Section 7.7.1 of [2].)
The status column has six defined values:
- `active', which indicates that the conceptual row is available for use by the managed device;
- `notInService', which indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device (see NOTE below);
- `notReady', which indicates that the conceptual row exists in the agent, but is missing information necessary in order to be available for use by the managed device;
- `createAndGo', which is supplied by a management station wishing to create a new instance of a conceptual row and to have its status automatically set to active, making it available for use by the managed device;
- `createAndWait', which is supplied by a management station wishing to create a new instance of a conceptual row (but not make it available for use by the managed device); and,
- `destroy', which is supplied by a management station wishing to delete all of the instances associated with an existing conceptual row.
Whereas five of the six values (all except `notReady') may be specified in a management protocol set operation, only three values will be returned in response to a management protocol retrieval operation: `notReady', `notInService' or `active'. That is, when queried, an existing conceptual row has only three states: it is either available for use by the managed device (the status column has value `active'); it is not available for use by the managed device, though the agent has sufficient information to make it so (the status column has value `notInService'); or, it is not available for use by the managed device, and an attempt to make it so would fail because the agent has insufficient information (the state column has value `notReady').
NOTE WELL
This textual convention may be used for a MIB table, irrespective of whether the values of that table's conceptual rows are able to be modified while it is active, or whether its conceptual rows must be taken out of service in order to be modified. That is, it is the responsibility of the DESCRIPTION clause of the status column to specify whether the status column must not be `active' in order for the value of some other column of the same conceptual row to be modified. If such a specification is made, affected columns may be changed by an SNMP set PDU if the RowStatus would not be equal to `active' either immediately before or after processing the PDU. In other words, if the PDU also contained a varbind that would change the RowStatus value, the column in question may be changed if the RowStatus was not equal to `active' as the PDU was received, or if the varbind sets the status to a value other than 'active'.
Also note that whenever any elements of a row exist, the RowStatus column must also exist.
To summarize the effect of having a conceptual row with a status column having a SYNTAX clause value of RowStatus, consider the following state diagram:

STATE

A	B	C	D
ACTION	does not exist	notReady	notInService	is active
set status column to createAndGo	noError -> D	inconsistentValue	inconsistentValue	inconsistentValue
set status column to createAndWait	noError see 1	inconsistentValue	inconsistentValue	inconsistentValue
set status column to active	inconsistentValue	inconsistentValue	noError see 2 -> D	noError -> D
set status column to notInService	inconsistentValue	inconsistentValue	noError see 3 -> C	noError -> C
set status column to destroy	noError -> A	noError -> A	noError -> A	noError -> A
set any other column to some value	see 4	noError see 1	noError -> C	see 5 -> D

(1) goto B or C, depending on information available to the agent.
(2) if other variable bindings included in the same PDU, provide values for all columns which are missing but required, then return noError and goto D.
(3) if other variable bindings included in the same PDU, provide values for all columns which are missing but required, then return noError and goto C.
(4) at the discretion of the agent, the return value may be either:
inconsistentName: because the agent does not choose to create such an instance when the corresponding RowStatus instance does not exist, or
inconsistentValue: if the supplied value is inconsistent with the state of some other MIB object's value, or
noError: because the agent chooses to create the instance.
If noError is returned, then the instance of the status column must also be created, and the new state is B or C, depending on the information available to the agent. If inconsistentName or inconsistentValue is returned, the row remains in state A.
(5) depending on the MIB definition for the column/table, either noError or inconsistentValue may be returned.
NOTE: Other processing of the set request may result in a response other than noError being returned, e.g., wrongValue, noCreation, etc.

Conceptual Row Creation

There are four potential interactions when creating a conceptual row: selecting an instance-identifier which is not in use; creating the conceptual row; initializing any objects for which the agent does not supply a default; and,

making the conceptual row available for use by the managed device.

Interaction 1: Selecting an Instance-Identifier

The algorithm used to select an instance-identifier varies for each conceptual row. In some cases, the instance-identifier is semantically significant, e.g., the destination address of a route, and a management station selects the instance-identifier according to the semantics. In other cases, the instance-identifier is used solely to distinguish conceptual rows, and a management station without specific knowledge of the conceptual row might examine the instances present in order to determine an unused instance-identifier. (This approach may be used, but it is often highly sub-optimal; however, it is also a questionable practice for a naive management station to attempt conceptual row creation.)

Alternately, the MIB module which defines the conceptual row might provide one or more objects which provide assistance in determining an unused instance-identifier. For example, if the conceptual row is indexed by an integer-value, then an object having an integer-valued SYNTAX clause might be defined for such a purpose, allowing a management station to issue a management protocol retrieval operation. In order to avoid unnecessary collisions between competing management stations, `adjacent' retrievals of this object should be different.

Finally, the management station could select a pseudo-random number to use as the index. In the event that this index was already in use and an inconsistentValue was returned in response to the management protocol set operation, the management station should simply select a new pseudo-random number and retry the operation.

A MIB designer should choose between the two latter algorithms based on the size of the table (and therefore the efficiency of each algorithm). For tables in which a large number of entries are expected, it is recommended that a MIB object be defined that returns an acceptable index for creation. For tables with small numbers of entries, it is recommended that the latter pseudo-random index mechanism be used.

Interaction 2: Creating the Conceptual Row

Once an unused instance-identifier has been selected, the management station determines if it wishes to create and activate the conceptual row in one transaction or in a negotiated set of interactions.

Interaction 2a: Creating and Activating the Conceptual Row

The management station must first determine the column requirements, i.e., it must determine those columns for which it must or must not provide values. Depending on the complexity of the table and the management station's knowledge of the agent's capabilities, this determination can be made locally by the management station. Alternately, the management station issues a management protocol get operation to examine all columns in the conceptual row that it wishes to create. In response, for each column, there are three possible outcomes:

- a value is returned, indicating that some other management station has already created this conceptual row. We return to interaction 1.
- the exception `noSuchInstance' is returned, indicating that the agent implements the object-type associated with this column, and that this column in at least one conceptual row would be accessible in the MIB view used by the retrieval were it to exist. For those columns to which the agent provides read-create access, the `noSuchInstance' exception tells the management station that it should supply a value for this column when the conceptual row is to be created.
- the exception `noSuchObject' is returned, indicating that the agent does not implement the object-type associated with this column or that there is no

conceptual row for which this column would be accessible in the MIB view used by the retrieval. As such, the management station can not issue any management protocol set operations to create an instance of this column.

Once the column requirements have been determined, a management protocol set operation is accordingly issued. This operation also sets the new instance of the status column to `createAndGo'.

When the agent processes the set operation, it verifies that it has sufficient information to make the conceptual row available for use by the managed device. The information available to the agent is provided by two sources: the management protocol set operation which creates the conceptual row, and, implementation-specific defaults supplied by the agent (note that an agent must provide implementation-specific defaults for at least those objects which it implements as read-only). If there is sufficient information available, then the conceptual row is created, a `noError' response is returned, the status column is set to `active', and no further interactions are necessary (i.e., interactions 3 and 4 are skipped). If there is insufficient information, then the conceptual row is not created, and the set operation fails with an error of `inconsistentValue'.

On this error, the management station can issue a management protocol retrieval operation to determine if this was because it failed to specify a value for a required column, or, because the selected instance of the status column already existed. In the latter case, we return to interaction 1. In the former case, the management station can re-issue the set operation with the additional information, or begin interaction 2 again using `createAndWait' in order to negotiate creation of the conceptual row.

NOTE WELL

Regardless of the method used to determine the column requirements, it is possible that the management station might deem a column necessary when, in fact, the agent will not allow that particular columnar instance to be created or written. In this case, the management protocol set operation will fail with an error such as `noCreation' or `notWritable'. In this case, the management station decides whether it needs to be able to set a value for that particular columnar instance. If not, the management station re-issues the management protocol set operation, but without setting a value for that particular columnar instance; otherwise, the management station aborts the row creation algorithm.

Interaction 2b: Negotiating the Creation of the Conceptual Row

The management station issues a management protocol set operation which sets the desired instance of the status column to `createAndWait'. If the agent is unwilling to process a request of this sort, the set operation fails with an error of `wrongValue'. (As a consequence, such an agent must be prepared to accept a single management protocol set operation, i.e., interaction 2a above, containing all of the columns indicated by its column requirements.) Otherwise, the conceptual row is created, a `noError' response is returned, and the status column is immediately set to either `notInService' or `notReady', depending on whether it has sufficient information to make the conceptual row available for use by the managed device. If there is sufficient information available, then the status column is set to `notInService'; otherwise, if there is insufficient information, then the status column is set to `notReady'. Regardless, we proceed to interaction 3.

Interaction 3: Initializing non-defaulted Objects

The management station must now determine the column requirements. It issues a management protocol get operation

to examine all columns in the created conceptual row. In the response, for each column, there are three possible outcomes:
- a value is returned, indicating that the agent implements the object-type associated with this column and had sufficient information to provide a value. For those columns to which the agent provides read-create access (and for which the agent allows their values to be changed after their creation), a value return tells the management station that it may issue additional management protocol set operations, if it desires, in order to change the value associated with this column.
- the exception `noSuchInstance' is returned, indicating that the agent implements the object-type associated with this column, and that this column in at least one conceptual row would be accessible in the MIB view used by the retrieval were it to exist. However, the agent does not have sufficient information to provide a value, and until a value is provided, the conceptual row may not be made available for use by the managed device. For those columns to which the agent provides read-create access, the `noSuchInstance' exception tells the management station that it must issue additional management protocol set operations, in order to provide a value associated with this column.
- the exception `noSuchObject' is returned, indicating that the agent does not implement the object-type associated with this column or that there is no conceptual row for which this column would be accessible in the MIB view used by the retrieval. As such, the management station can not issue any management protocol set operations to create an instance of this column.

If the value associated with the status column is `notReady', then the management station must first deal with all `noSuchInstance' columns, if any. Having done so, the value of the status column becomes `notInService', and we proceed to interaction 4.

Interaction 4: Making the Conceptual Row Available

Once the management station is satisfied with the values associated with the columns of the conceptual row, it issues a management protocol set operation to set the status column to `active'. If the agent has sufficient information to make the conceptual row available for use by the managed device, the management protocol set operation succeeds (a `noError' response is returned). Otherwise, the management protocol set operation fails with an error of `inconsistentValue'.

NOTE WELL

A conceptual row having a status column with value `notInService' or `notReady' is unavailable to the managed device. As such, it is possible for the managed device to create its own instances during the time between the management protocol set operation which sets the status column to `createAndWait' and the management protocol set operation which sets the status column to `active'. In this case, when the management protocol set operation is issued to set the status column to `active', the values held in the agent supersede those used by the managed device.

If the management station is prevented from setting the status column to `active' (e.g., due to management station or network failure) the conceptual row will be left in the `notInService' or `notReady' state, consuming resources indefinitely. The agent must detect conceptual rows that have been in either state for an abnormally long period of time and remove them. It is the responsibility of the DESCRIPTION clause of the status column to indicate what an abnormally long period of time would be. This period of time should be long enough to allow for human response time (including `think time') between the creation of the

	conceptual row and the setting of the status to `active'. In the absense of such information in the DESCRIPTION clause, it is suggested that this period be approximately 5 minutes in length. This removal action applies not only to newly-created rows, but also to previously active rows which are set to, and left in, the notInService state for a prolonged period exceeding that which is considered normal for such a conceptual row. Conceptual Row Suspension When a conceptual row is `active', the management station may issue a management protocol set operation which sets the instance of the status column to `notInService'. If the agent is unwilling to do so, the set operation fails with an error of `wrongValue'. Otherwise, the conceptual row is taken out of service, and a `noError' response is returned. It is the responsibility of the DESCRIPTION clause of the status column to indicate under what circumstances the status column should be taken out of service (e.g., in order for the value of some other column of the same conceptual row to be modified). Conceptual Row Deletion For deletion of conceptual rows, a management protocol set operation is issued which sets the instance of the status column to `destroy'. This request may be made regardless of the current value of the status column (e.g., it is possible to delete conceptual rows which are either `notReady', `notInService' or `active'.) If the operation succeeds, then all instances associated with the conceptual row are immediately removed.
cTap2MediationContentId	cTap2MediationContentId is a session identifier, from the intercept application's perspective, and a content identifier from the Mediation Device's perspective. The Mediation Device is responsible for making sure these are unique, although the SNMP RowStatus row creation process will help by not allowing it to create conflicting entries. Before creating a new entry, a value for this variable may be obtained by reading cTap2MediationNewIndex to reduce the probability of a value collision.

Go Top

SECTION 12.47

Trap: ciscoNtpGeneralConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with all NTP servers is lost	NtpConnectionState	SGW
NtpConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with NTP server has been restored	NtpConnectionState	SGW

Description:

```
This trap is sent when the device loses connectivity            to all NTP servers.
```

Default Message:

$NodeDisplayName - Connection with all NTP servers is lost.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 12.48

Trap: ciscoNtpHighPriorityConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with the high priority NTP server is failed	NtpHighPriorityConnectionState	SGW
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with the high priority NTP server is restored	NtpHighPriorityConnectionState	SGW

Description:

```
A failure to connect with an high priority NTP server (e.g. a server at the lowest stratum) is detected.
```

Default Message:

$NodeDisplayName - Connection with the high priority NTP server is failed

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpPeersPeerAddress	The IP address of the peer. When creating a new association, a value should be set either for this object or the corresponding instance of cntpPeersPeerName, before the row is made active.
cntpPeersAssocId	An integer value greater than 0 that uniquely identifies a peer with which the local NTP server is associated.

Go Top

SECTION 12.49

Trap: ciscoNtpSrvStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpServerStatus	Trap	Alarm	Yes	Indeterminate	$NodeDisplayName - The NTP server status is unknown	NtpServerStatus	SGW
NtpServerStatus	Trap	Alarm	Yes	Critical	$NodeDisplayName - The NTP server is not running	NtpServerStatus	SGW
NtpServerStatus	Trap	Alarm	Yes	Warning	$NodeDisplayName - The NTP server is not synchronized to any time source	NtpServerStatus	SGW
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to its own local clock	NtpServerStatus	SGW
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a local hardware refclock	NtpServerStatus	SGW
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a remote NTP server	NtpServerStatus	SGW

Description:

```
This notification is generated whenever the value of cntpSysSrvStatus changes.
```

Default Message:

$NodeDisplayName - The NTP server status is unknown
$NodeDisplayName - The NTP server is not running
$NodeDisplayName - The NTP server is not synchronized to any time source
$NodeDisplayName - The NTP server is synchronized to its own local clock
$NodeDisplayName - The NTP server is synchronized to a local hardware refclock

$NodeDisplayName - The NTP server is synchronized to a remote NTP server

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpSysSrvStatus	Current state of the NTP server with values coded as follows: 1: server status is unknown 2: server is not running 3: server is not synchronized to any time source 4: server is synchronized to its own local clock 5: server is synchronized to a local hardware refclock (e.g. GPS) 6: server is synchronized to a remote NTP server INTEGER is unknown

Go Top

SECTION 12.50

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is above the high threshold of $GGSNHighThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	SGW
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	SGW
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is below the low threshold of $GGSNLowThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	SGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent

	throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.

width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 12.51

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is above the high threshold of $GGSNHighThreshold percent of total signalling messages received.	GTPUnexpectedMsgsThreshold	SGW
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total signalling messages received.	GTPUnexpectedMsgsThreshold	SGW
					$NodeDisplayName - The number of unexpected signalling messages received is		

GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Normal	$GGSNThresholdValue percent of total signalling messages received which is below the low threshold of $GGSNLowThreshold percent of the total signalling messages received.	GTPUnexpectedMsgsThreshold	SGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This

	alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 12.52

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is above the high threshold of $GGSNHighThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	SGW
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	SGW
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is below the low threshold of $GGSNLowThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	SGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	Alarm Description
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the

Roman";">IPOutboundNoRoutesThreshold	number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 12.53

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is above the high threshold of $GGSNHighThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	SGW
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	SGW
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is below the low threshold of $GGSNLowThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	SGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	Alarm Description
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 12.54

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is above the high threshold of $GGSNHighThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	SGW
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	SGW
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is below the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	SGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes

	received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.

width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 12.55

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is above the high threshold of $GGSNHighThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	SGW
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	SGW
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is below the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	SGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**

width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.

width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 12.56

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is above the high threshold of $GGSNHighThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	SGW
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	SGW
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is below the low threshold of $GGSNLowThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	SGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams

	exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 12.57

Trap: ciscoIpLocalPoolInUseAddrNoti

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	SGW
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold abated. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	SGW
IPLocalPoolThreshold	Trap	Event	No	Informational	$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .	IPLocalPoolThreshold	SGW

Description:

A notification indicating that number of used addresses of an IP local pool exceeded the threshold value indicated by cIpLocalPoolStatInUseAddrThldHi.

Default Message:

$NodeDisplayName - IP local pool threshold exceeded. Used addresses = $cIpLocalPoolStatInUseAddrs. Available addresses = $cIpLocalPoolStatFreeAddrs .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIpLocalPoolStatFreeAddrs	The number of IP addresses available for use in this IP local pool.
cIpLocalPoolStatInUseAddrs	The number of IP addresses being used in this IP local pool.

Go Top

SECTION 12.58

Trap: ciscoTap2MIBActive

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MIBActive	Trap	Event	No	Informational	$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.	Tap2MIBActive	SGW

Description:

```
This Notification is sent when an intercepting router or       switch is first capable of intercepting a packet corresponding
to a configured data stream. The value of the corresponding
cTap2StreamType which identifies the actual intercept stream
type is included in this notification.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.  Filter
installation can take a long period of time, during which call
progress may be delayed.
```

Default Message:

$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 12.59

Trap: ciscoTap2MediationDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .	Tap2MediationDebug	SGW

Description:

```
When there is intervention needed due to some events related       to entries configured in cTap2MediationTable, the device
notifies the manager of the event.
This notification may be generated in conjunction with the
```

```
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.
```

Default Message:

$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 12.60

Trap: ciscoTap2StreamDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2StreamDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId	Tap2StreamDebug	SGW

Description:

```
When there is intervention needed due to some events related        to entries configured in cTap2StreamTable, the device
notifies the manager of the event.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.
```

Default Message:

$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId.br>

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.

cTap2DebugStreamId	The value of this object is that of cTap2StreamIndex of an entry in cTap2StreamTable. This object along with cTap2DebugMediationId identifies an entry in cTap2StreamTable. The value of this object may be zero, in which this debug message is regarding a Mediation Device, but not a particular stream. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2StreamTable fails.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 12.61

Trap: ciscoTap2Switchover

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2Switchover	Trap	Event	No	Informational	$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.	Tap2Switchover	SGW

Description:

```
This notification is sent when there is a redundant (standby)       route processor available on the intercepting device and the
current active processor is going down causing standby to
takeover. Note that this notification may be sent by the
intercepting device only when it had a chance to know before it
goes down.
Mediation device when received this notification should assume
that configured intercepts on the intercepting device no longer
exist, when the standby processor takes control. This means that
the Mediation device should again configure the intercepts.
```

Default Message:

$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 12.62

Status: ApnInstanceStateAdded and ApnInstanceStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceState	Poll	Event	No	Normal	APN $ApnDisplayName on gateway $NodeDisplayName added in state Active/ActiveReason.	ApnInstanceState	SGW
ApnInstanceState	Poll	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName added in state $ApnInstanceState/$ApnInstanceStateReason.	ApnInstanceState	SGW
ApnInstanceState	Poll	Event	No	Normal	APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to Active/ActiveReason.	ApnInstanceState	SGW
ApnInstanceState	Poll	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to $ApnInstanceState/$ApnInstanceStateReason.	ApnInstanceState	SGW

Description:

The ApnInstanceStateAdded and ApnInstanceStateChanged status eventsprovide information when an ApnInstance object is added to the MWTM object model or when MWTM detects that the state of an ApnInstance has changed. An ApnInstance is defined as an access-point and accesspoint-name defined on a gateway router. An ApnInstance object is located under the gateway Node object in the MWTM object tree. The value of ApnInstanceState indicates the new state. Possible values of ApnInstanceState include:

- Active - Traffic may flow over this ApnInstance.
- Unknown - The attempt to determine the state of the ApnInstance failed.
- Warning - The ApnInstance is Active however some underlying status contributor of this ApnInstance is not fully functional.
- Deleted - The ApnInstance has been deleted from the object database.

Default Message:

- APN $ApnDisplayName on gateway $NodeDisplayName added in state $ApnInstanceState/$ApnInstanceStateReason.
- APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to $ApnInstanceState/$ApnInstanceStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
ApnInstanceState	The current state of the ApnInstance.
ApnInstanceStateReason	The current state reason of of the ApnInstance.
ApnInstanceLastState	The previous state of the ApnInstance.

Operational Information:

See also:

Go Top

SECTION 12.63

Status: ApnStateAdded and ApnStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnState	Poll	Event	No	Normal	APN $ApnDisplayName added in state Active/ActiveReason.	ApnState	SGW
ApnState	Poll	Event	No	Informational	APN $ApnDisplayName added in state $ApnState/$ApnStateReason.	ApnState	SGW
ApnState	Poll	Event	No	Normal	APN $ApnDisplayName changed state from $ApnLastState to Active/ActiveReason.	ApnState	SGW
ApnState	Poll	Event	No	Informational	APN $ApnDisplayName changed state from $ApnLastState to $ApnState/$ApnStateReason.	ApnState	SGW

Description:

The ApnStateAdded and ApnStateChanged status events provideinformation when an Apn object is added to the MWTM object model or when MWTM detects that the state of an Apn has changed. An Apn is defined as an aggregation of a set of ApnInstance objects defined across a set of gateway routers. An Apn object is located as a top level object in the MWTM object tree. The value of ApnState indicates the new state. Possible values of ApnState include:

- Active - Traffic may flow over this Apn.
- Warning - The Apn is Active however one or more of its constituent ApnInstances is not fully functional.

- Deleted - The Apn has been deleted from the object database.

Default Message:

- Apn $ApnDisplayName added in state $ApnState/$ApnStateReason.
- Apn $ApnDisplayName changed state from $ApnLastState to $ApnState/$ApnStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
ApnState	The current state of the Apn.
ApnStateReason	The current state reason of of the Apn.
ApnLastState	The previous state of the Apn.

Operational Information:

See also:

Go Top

SECTION 12.64

UserAction: ApnInstanceIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceIgnoredSet	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.	ApnInstanceIgnoredSet	SGW

Description:

The ApnInstanceIgnoredSet UserAction event provides information when a ApnInstance's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the ApnInstance in the aggregation algorithm in determining the state of a Node or Apn. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The ApnInstance is to be excluded from state aggregation.
- False - The ApnInstance is to be included in state aggregation.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
ApnInstanceState	The current state of the ApnInstance.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the ApnInstances which are currently ignored select the ApnInstance folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 12.65

UserAction: ApnIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnIgnoredSet	User Action	Event	No	Informational	APN $ApnDisplayName ignore flag is set to $IgnoredFlag by $User.	ApnIgnoredSet	SGW

Description:

The ApnIgnoredSet UserAction event provides information when a Apn's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the Apn in the aggregation algorithm in determining the state of higher level objects. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The Apn is to be excluded from state aggregation.
- False - The Apn is to be included in state aggregation.

Default Message:

APN $ApnDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
ApnState	The current state of the Apn.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the Apns which are currently ignored select the Apn folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 12.66

UserAction: ApnInstanceUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceUserDataUpdated	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName edited by user $User.	ApnInstanceUserDataUpdated	SGW

Description:

The ApnInstanceUserDataUpdated UserAction event provides information when a ApnInstance object's user data has been updated by a MWTM user.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName edited by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
User	The user who requested the ApnInstance's data be updated.

Operational Information:

The fields that can be updated for a ApnInstance include:

- The ApnInstance's notes data used for communicating installation dependent information about a ApnInstance.

Go Top

SECTION 12.67

UserAction: ApnUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnUserDataUpdated	User Action	Event	No	Informational	APN $ApnDisplayName edited by user $User.	ApnUserDataUpdated	SGW

Description:

The ApnUserDataUpdated UserAction event provides information when a Apn object's user data has been updated by a MWTM user.

Default Message:

APN $ApnDisplayName edited by user $User.

Message Substitution Variables:

Node
Substitution variables for Node related data.

ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
User	The user who requested the Apn's data be updated.

Operational Information:

The fields that can be updated for a Apn include:

- The Apn's notes data used for communicating installation dependent information about a Apn.

Go Top

SECTION 12.68

UserAction: ApnInstanceDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceDeleted	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName deleted by user $User.	ApnInstanceDeleted	SGW

Description:

The ApnInstanceDeleted UserAction event provides information when a ApnInstanceobject's deletion from the MWTM object model database is requested.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName deleted by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
User	The user who requested the ApnInstance's data be deleted.

Operational Information:

- The deletion of a ApnInstance can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 12.69

UserAction: ApnDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnDeleted	User Action	Event	No	Informational	APN $ApnDisplayName deleted by user $User.	ApnDeleted	SGW

Description:

The ApnDeleted UserAction event provides information when a Apnobject's deletion from the MWTM object model database is requested.

Default Message:

APN $ApnDisplayName deleted by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
User	The user who requested the Apn's data be deleted.

Operational Information:

- The deletion of a Apn can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 13.1

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigModified	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was modified.	APN-ConfigModified	SPGW

Description:

```
A notification of this type is generated when an              entry is generated in the
cgprsAccPtCfgNotifHistTable and
cgprsAccPtCfgNotifEnable is set to true.
```

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 13.2

Trap: cgprsAccPtMaintenanceNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ServiceMode	Trap	Alarm	Yes	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in maintenance mode.	APN-ServiceMode	SPGW
APN-ServiceMode	Trap	Alarm	Yes	Normal	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in service.	APN-ServiceMode	SPGW
APN-ServiceMode	Poll	Alarm	Yes	Major	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in maintenance mode.	APN-ServiceMode	SPGW
APN-ServiceMode	Poll	Alarm	Yes	Normal	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN is in service.	APN-ServiceMode	SPGW

Description:

A notification of this type is generated when APN is placed in maintenance mode which is specified by cgprsAccPtOperationMode.

Default Message:

$NodeDisplayName -- The APN ($cgprsAccPtCfgNotifAccPtIndex) is in maintenance mode.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.

Go Top

SECTION 13.3

Trap: cgprsCgGatewayGroupInServiceModeNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	SPGW
ChargingGatewayMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	SPGW
ChargingGatewayMaintenanceMode	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The charging gateway is in service.	ChargingGatewayMaintenanceMode	SPGW
ChargingGatewayMaintenanceMode	Poll	Alarm	Yes	Warning	$NodeDisplayName -- The charging gateway is in maintenance mode.	ChargingGatewayMaintenanceMode	SPGW

Description:

```
The cgprsCgGatewayGroupInServiceModeNotif notification is        generated when the charging group state transitions to
in-service mode, identified by the object
cgprsCgGroupServiceMode
```

Default Message:

$NodeDisplayName -- The charging gateway is in service.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgGroupServiceMode	This object specifies the charging service-mode for a charging group. The charging functions in the GGSN involve mainly collection/accumulation of CDRs and transmitting CDRs to the Charging Gateways. The charging service-mode function has no impact to the collection/accumulation of CDRs. The charging service mode function only involves the transmission of CDRs to the charging gateways. The charging service-mode has the following two states: 'operational' : In this state, the charging group will observe normal charging operations. That is, accumulation and transmission of CDRs to the charging gateway will continue as is done normally. 'maintenance' : In this state, transmission of CDRs to the charging gateways will not be performed; However, collection and accumulation of CDRs will continue as is done normally. When the GGSN is in 'maintenance' mode, all the charging configurations will be allowed. In the system-init phase, the charging service mode CLI configs will not be handled. The handling of 'Redirecting Request', 'Node Alive' and charging gateway switchover mechanisms will not be performed while the charging is in maintenance mode. After the mode is changed to operational mode, the messages in the pending queue will be sent towards the newly configured active charging gateway and the normal functions will continue from thereon. When switching between modes, traps will be generated using cgprsCgGatewayGroupInServiceModeNotif and cgprsCgGatewayGroupMaintenanceModeNotif. INTEGER is unknown
cgprsCgGroupIndex	A locally unique identifier for the charging groups on GGSN. Note: There is support for only 30 charging groups (0-29). Where charging group 0 is also referred as default charging gateway group.

Go Top

SECTION 13.4

Trap: cgprsCgGatewayGroupAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayState	Trap	Alarm	Yes	Critical	$NodeDisplayName - The Charging gateway is down	ChargingGatewayState	SPGW
ChargingGatewayState	Trap	Alarm	Yes	Normal	$NodeDisplayName - The Charging gateway is up	ChargingGatewayState	SPGW

Description:

```
A cgprsCgGroupAlarmNotif signifies that a GPRS related       alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgGatewayGroupAlarmHistTable.
```

Default Message:

$NodeDisplayName . The Charging gateway is down
$NodeDisplayName . The charging gateway is up
$NodeDisplayName . The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.
$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- The gateway received an echo response from the charging gateway.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgGatewayGroupAlarmHistType	This object indicates the type of GPRS, charging gateway or charging related alarm. Identifies the possible types of GPRS charging gateway and charging related alarm. cgprsCgAlarmCgDown - CG is down. cgprsCgAlarmCgUp - CG is up. cgprsCgAlarmTransFailure - The GGSN has repeatedly failed to receive responses for Data Record Transfer Request Messages from CG. cgprsCgAlarmTransSuccess - The GGSN has successfully sent Data Record Transfer Request Message to CG after the failure. cgprsCgAlarmCapacityFull - The GGSN is out of memory and has failed to buffer a G-CDR internally. cgprsCgAlarmCapacityFree - The GGSN is able to buffer G-CDR after the failure to buffer G-CDRs. cgprsCgAlarmEchoFailure - The GGSN has repeatedly failed to receive the Echo Response Messages from the CG for the Echo Request message. cgprsCgAlarmEchoRestored - The GGSN has got the Echo Response from the CG after the cgprsCgAlarmEchoFailure has been detected. cgprsCgAlarmCdrDiscard - The G-CDRs are discarded. cgprsCgAlarmCdrDiscardRestored - This is to indicate that GGSN has started buffering G-CDRs after cgprsCgAlarmCdrDiscard has occured. cgprsCgAlarmChargingDisabled - Indicates that charging transactions on the GGSN are disabled. cgprsCgAlarmChargingEnabled - Indicates that charging transactions on the GGSN

	are enabled.
cgprsCgGatewayGroupAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgGatewayGroupAlarmHistAddress. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cgprsCgGatewayGroupAlarmHistSeverity	This object indicates the severity of the alarm. Represents the perceived alarm severity associated with a service or safety affecting condition and/or event. These are based on ITU severities, except that info(7) is added. cleared(1) - Indicates a previous alarm condition has been cleared. It is not required (unless specifically stated elsewhere on a case by case basis) that an alarm condition that has been cleared will produce a notification or other event containing an alarm severity with this value. indeterminate(2) - Indicates that the severity level cannot be determined. critical(3) - Indicates that a service or safety affecting condition has occurred and an immediate corrective action is required. major(4) - Indicates that a service affecting condition has occurred and an urgent corrective action is required. minor(5) - Indicates the existence of a non-service affecting condition and that corrective action should be taken in order to prevent a more serious (for example, service or safety affecting) condition. warning(6) - Indicates the detection of a potential or impending service or safety affecting condition, before any significant effects have been felt. info(7) -

	Indicates an alarm condition that does not meet any other severity definition. This can include important, but non-urgent, notices or informational events.
cgprsCgGatewayGroupAlarmHistAddress	This object indicates the IP address that is used to uniquely identify the CG.
cgprsCgGatewayGroupAlarmHistInfo	This object provides detailed information when a GPRS charging gateway or charging related alarm is generated.
cgprsCgGroupIndex	A locally unique identifier for the charging groups on GGSN. Note: There is support for only 30 charging groups (0-29). Where charging group 0 is also referred as default charging gateway group.
cgprsCgGatewayGroupAlarmHistIndex	This object indicates a monotonically increasing integer for the sole purpose of indexing the charging gateway and charging related alarms in a charging group. When the index reaches the maximum value it will wrap around to one.

Go Top

SECTION 13.5

Trap: cgprsCgGatewayGroupSwitchoverNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewaySwitchover	Trap	Alarm	No	Major	$NodeDisplayName -- The charging gateway switched from $cgprsCgGatewayGroupStatusOldCgAddr to $cgprsCgGatewayGroupStatusActiveCgAddr	ChargingGatewaySwitchover	SPGW

Description:

```
A notification of this type is generated when the        charging gateway is switched, the new charging
gateway is identified by cgprsCgGatewayGroupStatusActiveCgAddr
and the old charging gateway is identified by
cgprsCgGatewayGroupStatusOldCgAddr.
```

Default Message:

$NodeDisplayName -- The charging gateway switched from $cgprsCgGatewayGroupStatusOldCgAddr to $cgprsCgGatewayGroupStatusActiveCgAddr.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgGatewayGroupStatusAddrType	This object indicates the address type of the active charging gateway. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention.

	ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cgprsCgGatewayGroupStatusActiveCgAddr	This object indicates the address of the active charging gateway. The type of address will be represented by cgprsCgGatewayGroupStatusAddrType
cgprsCgGatewayGroupStatusOldCgAddr	This object indicates the address of the previous active charging gateway. The type of address will same as the one present in cgprsCgGatewayGroupStatusAddrType.
cgprsCgGroupIndex	A locally unique identifier for the charging groups on GGSN. Note: There is support for only 30 charging groups (0-29). Where charging group 0 is also referred as default charging gateway group.

Go Top

SECTION 13.6

Trap: cGtpPathFailedNotification

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPPathFailed	Trap	Alarm	No	Major	$NodeDisplayName -- Peer ($cGtpLastNoRespToEchoGSNIpAddr) failed to respond to the GTP Echo Request.	GTPPathFailed	SPGW

Description:

```
This notification is sent when one of this GSN's peers           failed to respond to the GTP 'Echo Request' message for
the waiting interval.
```

Default Message:

$NodeDisplayName -- Peer ($cGtpLastNoRespToEchoGSNIpAddr) failed to respond to the GTP Echo Request.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGtpLastNoRespToEchoGSNIpAddrTyp	This object indicates the type of Internet address by which cGtpLastNoRespToEchoGSNIpAddr is reachable.

cGtpLastNoRespToEchoGSNIpAddr	The IP address of the last peer GSN device that did not reply to an GTP 'Echo Request' message from the local GSN device.

Go Top

SECTION 13.7

Trap: cGgsnMaintenanceNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GWMaintenanceMode	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is in maintenance mode.	GWMaintenanceMode	SPGW
GWMaintenanceMode	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is in service.	GWMaintenanceMode	SPGW
GWMaintenanceMode	Poll	Alarm	Yes	Major	$NodeDisplayName -- The gateway is in maintenance mode.	GWMaintenanceMode	SPGW
GWMaintenanceMode	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is in service.	GWMaintenanceMode	SPGW

Description:

A notification of this type is generated when the gateway is placed in maintenance mode which is specified by cGgsnServiceModeStatus.

Default Message:

$NodeDisplayName -- The gateway is in maintenance mode.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 13.8

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigCreated	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was created.	APN-ConfigCreated	SPGW

Description:

A notification of this type is generated when an entry is generated in the cgprsAccPtCfgNotifHistTable and cgprsAccPtCfgNotifEnable is set to true.

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router

	that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 13.9

Trap: cgprsAccPtCfgNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
APN-ConfigDeleted	Trap	Alarm	No	Warning	APN $ApnDisplayName on gateway $NodeDisplayName -- The APN configuration was deleted.	APN-ConfigDeleted	SPGW

Description:

A notification of this type is generated when an entry is generated in the cgprsAccPtCfgNotifHistTable and cgprsAccPtCfgNotifEnable is set to true.

Default Message:

$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been created.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been deleted.
$NodeDisplayName -- The Access Point ($cgprsAccPtCfgNotifAccPtIndex) configuration has been modified.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsAccPtCfgNotifAccPtIndex	This object specifies the access point which has been created, changed or modified.
cgprsAccPtCfgNotifReason	This object describes the reason of the notification.

Go Top

SECTION 13.10

Trap: cgprsCgGatewayGroupAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingTransferState	Trap	Alarm	Yes	Major	$NodeDisplayName - The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway	ChargingTransferState	SPGW
ChargingTransferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.	ChargingTransferState	SPGW

Description:

A cgprsCgGroupAlarmNotif signifies that a GPRS related alarm is detected in the managed system. This alarm is sent after an entry has been added to cgprsCgGatewayGroupAlarmHistTable.

Default Message:

$NodeDisplayName . The Charging gateway is down
$NodeDisplayName . The charging gateway is up
$NodeDisplayName . The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.
$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- The gateway received an echo response from the charging gateway.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgGatewayGroupAlarmHistType	This object indicates the type of GPRS, charging gateway or charging related alarm. Identifies the possible types of GPRS charging gateway and charging related alarm. cgprsCgAlarmCgDown - CG is down. cgprsCgAlarmCgUp - CG is up. cgprsCgAlarmTransFailure - The GGSN has repeatedly failed to receive responses for Data Record Transfer Request Messages from CG. cgprsCgAlarmTransSuccess - The GGSN has successfully sent Data Record Transfer Request Message to CG after the failure. cgprsCgAlarmCapacityFull - The GGSN is out of memory and has failed to buffer a G-CDR internally. cgprsCgAlarmCapacityFree - The GGSN is able to buffer G-CDR after the failure to buffer G-CDRs. cgprsCgAlarmEchoFailure - The GGSN has repeatedly failed to receive the Echo Response Messages from the CG for the Echo Request message. cgprsCgAlarmEchoRestored - The GGSN has got the Echo Response from the CG after the cgprsCgAlarmEchoFailure has been detected. cgprsCgAlarmCdrDiscard - The G-CDRs are discarded. cgprsCgAlarmCdrDiscardRestored - This is to indicate that GGSN has started buffering G-CDRs after cgprsCgAlarmCdrDiscard has occured. cgprsCgAlarmChargingDisabled - Indicates that charging transactions on the GGSN are disabled. cgprsCgAlarmChargingEnabled - Indicates that charging transactions on the GGSN are enabled.
cgprsCgGatewayGroupAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgGatewayGroupAlarmHistAddress. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding

	InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cgprsCgGatewayGroupAlarmHistSeverity	This object indicates the severity of the alarm. Represents the perceived alarm severity associated with a service or safety affecting condition and/or event. These are based on ITU severities, except that info(7) is added. cleared(1) - Indicates a previous alarm condition has been cleared. It is not required (unless specifically stated elsewhere on a case by case basis) that an alarm condition that has been cleared will produce a notification or other event containing an alarm severity with this value. indeterminate(2) - Indicates that the severity level cannot be determined. critical(3) - Indicates that a service or safety affecting condition has occurred and an immediate corrective action is required. major(4) - Indicates that a service affecting condition has occurred and an urgent corrective action is required. minor(5) - Indicates the existence of a non-service affecting condition and that corrective action should be taken in order to prevent a more serious (for example, service or safety affecting) condition. warning(6) - Indicates the detection of a potential or impending service or safety affecting condition, before any significant effects have been felt. info(7) - Indicates an alarm condition that does not meet any other severity definition. This can include important, but non-urgent, notices or informational events.
cgprsCgGatewayGroupAlarmHistAddress	This object indicates the IP address that is used to uniquely identify the CG.

cgprsCgGatewayGroupAlarmHistInfo	This object provides detailed information when a GPRS charging gateway or charging related alarm is generated.
cgprsCgGroupIndex	A locally unique identifier for the charging groups on GGSN. Note: There is support for only 30 charging groups (0-29). Where charging group 0 is also referred as default charging gateway group.
cgprsCgGatewayGroupAlarmHistIndex	This object indicates a monotonically increasing integer for the sole purpose of indexing the charging gateway and charging related alarms in a charging group. When the index reaches the maximum value it will wrap around to one.

Go Top

SECTION 13.11

Trap: cgprsCgGatewayGroupAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingCapacityState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.	ChargingCapacityState	SPGW
ChargingCapacityState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs	ChargingCapacityState	SPGW

Description:

```
A cgprsCgGroupAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgGatewayGroupAlarmHistTable.
```

Default Message:

$NodeDisplayName . The Charging gateway is down
$NodeDisplayName . The charging gateway is up
$NodeDisplayName . The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.
$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- The gateway received an echo response from the charging gateway.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgGatewayGroupAlarmHistType	This object indicates the type of GPRS, charging gateway or charging related alarm. Identifies the possible types of GPRS charging gateway and charging related alarm. cgprsCgAlarmCgDown - CG is down. cgprsCgAlarmCgUp - CG is up. cgprsCgAlarmTransFailure

	- The GGSN has repeatedly failed to receive responses for Data Record Transfer Request Messages from CG. cgprsCgAlarmTransSuccess - The GGSN has successfully sent Data Record Transfer Request Message to CG after the failure. cgprsCgAlarmCapacityFull - The GGSN is out of memory and has failed to buffer a G-CDR internally. cgprsCgAlarmCapacityFree - The GGSN is able to buffer G-CDR after the failure to buffer G-CDRs. cgprsCgAlarmEchoFailure - The GGSN has repeatedly failed to receive the Echo Response Messages from the CG for the Echo Request message. cgprsCgAlarmEchoRestored - The GGSN has got the Echo Response from the CG after the cgprsCgAlarmEchoFailure has been detected. cgprsCgAlarmCdrDiscard - The G-CDRs are discarded. cgprsCgAlarmCdrDiscardRestored - This is to indicate that GGSN has started buffering G-CDRs after cgprsCgAlarmCdrDiscard has occured. cgprsCgAlarmChargingDisabled - Indicates that charging transactions on the GGSN are disabled. cgprsCgAlarmChargingEnabled - Indicates that charging transactions on the GGSN are enabled.
cgprsCgGatewayGroupAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgGatewayGroupAlarmHistAddress. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cgprsCgGatewayGroupAlarmHistSeverity	This object indicates the severity of the alarm. Represents the perceived alarm severity associated with a service or safety affecting condition and/or event. These are based on ITU severities, except

	that info(7) is added. cleared(1) - Indicates a previous alarm condition has been cleared. It is not required (unless specifically stated elsewhere on a case by case basis) that an alarm condition that has been cleared will produce a notification or other event containing an alarm severity with this value. indeterminate(2) - Indicates that the severity level cannot be determined. critical(3) - Indicates that a service or safety affecting condition has occurred and an immediate corrective action is required. major(4) - Indicates that a service affecting condition has occurred and an urgent corrective action is required. minor(5) - Indicates the existence of a non-service affecting condition and that corrective action should be taken in order to prevent a more serious (for example, service or safety affecting) condition. warning(6) - Indicates the detection of a potential or impending service or safety affecting condition, before any significant effects have been felt. info(7) - Indicates an alarm condition that does not meet any other severity definition. This can include important, but non-urgent, notices or informational events.
cgprsCgGatewayGroupAlarmHistAddress	This object indicates the IP address that is used to uniquely identify the CG.
cgprsCgGatewayGroupAlarmHistInfo	This object provides detailed information when a GPRS charging gateway or charging related alarm is generated.
cgprsCgGroupIndex	A locally unique identifier for the charging groups on GGSN. Note: There is support for only 30 charging groups (0-29). Where charging group 0 is also referred as default charging gateway group.
cgprsCgGatewayGroupAlarmHistIndex	This object indicates a monotonically increasing integer for the sole purpose of indexing the charging gateway and charging related alarms in a charging group. When the index reaches the maximum value it will wrap around to one.

Go Top

SECTION 13.12

Trap: cgprsCgGatewayGroupAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingGatewayEchoState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.	ChargingGatewayEchoState	SPGW
ChargingGatewayEchoState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway received an echo response from the charging gateway.	ChargingGatewayEchoState	SPGW

Description:

```
A cgprsCgGroupAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgGatewayGroupAlarmHistTable.
```

Default Message:

$NodeDisplayName . The Charging gateway is down
$NodeDisplayName . The charging gateway is up
$NodeDisplayName . The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.
$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- The gateway received an echo response from the charging gateway.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgGatewayGroupAlarmHistType	This object indicates the type of GPRS, charging gateway or charging related alarm. Identifies the possible types of GPRS charging gateway and charging related alarm. cgprsCgAlarmCgDown - CG is down. cgprsCgAlarmCgUp - CG is up. cgprsCgAlarmTransFailure - The GGSN has repeatedly failed to receive responses for Data Record Transfer Request Messages from CG. cgprsCgAlarmTransSuccess - The GGSN has successfully sent Data Record Transfer Request Message to CG after the failure. cgprsCgAlarmCapacityFull - The GGSN is out of memory and has failed to buffer a G-CDR internally. cgprsCgAlarmCapacityFree - The GGSN is able to buffer G-CDR after the failure to buffer G-CDRs. cgprsCgAlarmEchoFailure - The GGSN has repeatedly failed to receive the Echo Response Messages from the CG for the Echo Request message. cgprsCgAlarmEchoRestored - The GGSN has got the Echo Response from the CG after the cgprsCgAlarmEchoFailure has been detected. cgprsCgAlarmCdrDiscard - The G-CDRs are discarded. cgprsCgAlarmCdrDiscardRestored - This is to indicate that GGSN has started buffering G-CDRs after cgprsCgAlarmCdrDiscard has occured. cgprsCgAlarmChargingDisabled - Indicates that charging transactions on the GGSN are disabled. cgprsCgAlarmChargingEnabled - Indicates that charging transactions on the GGSN are enabled.
cgprsCgGatewayGroupAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgGatewayGroupAlarmHistAddress. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding

	InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cgprsCgGatewayGroupAlarmHistSeverity	This object indicates the severity of the alarm. Represents the perceived alarm severity associated with a service or safety affecting condition and/or event. These are based on ITU severities, except that info(7) is added. cleared(1) - Indicates a previous alarm condition has been cleared. It is not required (unless specifically stated elsewhere on a case by case basis) that an alarm condition that has been cleared will produce a notification or other event containing an alarm severity with this value. indeterminate(2) - Indicates that the severity level cannot be determined. critical(3) - Indicates that a service or safety affecting condition has occurred and an immediate corrective action is required. major(4) - Indicates that a service affecting condition has occurred and an urgent corrective action is required. minor(5) - Indicates the existence of a non-service affecting condition and that corrective action should be taken in order to prevent a more serious (for example, service or safety affecting) condition. warning(6) - Indicates the detection of a potential or impending service or safety affecting condition, before any significant effects have been felt. info(7) - Indicates an alarm condition that does not meet any other severity definition. This can include important, but non-urgent, notices or informational events.
cgprsCgGatewayGroupAlarmHistAddress	This object indicates the IP address that is used to uniquely identify the CG.

cgprsCgGatewayGroupAlarmHistInfo	This object provides detailed information when a GPRS charging gateway or charging related alarm is generated.
cgprsCgGroupIndex	A locally unique identifier for the charging groups on GGSN. Note: There is support for only 30 charging groups (0-29). Where charging group 0 is also referred as default charging gateway group.
cgprsCgGatewayGroupAlarmHistIndex	This object indicates a monotonically increasing integer for the sole purpose of indexing the charging gateway and charging related alarms in a charging group. When the index reaches the maximum value it will wrap around to one.

Go Top

SECTION 13.13

Trap: cgprsCgGatewayGroupAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingCDRBufferState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The gateway has discarded G-CDRs.	ChargingCDRBufferState	SPGW
ChargingCDRBufferState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.	ChargingCDRBufferState	SPGW

Description:

```
A cgprsCgGroupAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgGatewayGroupAlarmHistTable.
```

Default Message:

$NodeDisplayName . The Charging gateway is down
$NodeDisplayName . The charging gateway is up
$NodeDisplayName . The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.
$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- The gateway received an echo response from the charging gateway.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgGatewayGroupAlarmHistType	This object indicates the type of GPRS, charging gateway or charging related alarm. Identifies the possible types of GPRS charging gateway and charging related alarm. cgprsCgAlarmCgDown - CG is down. cgprsCgAlarmCgUp - CG is up. cgprsCgAlarmTransFailure

	- The GGSN has repeatedly failed to receive responses for Data Record Transfer Request Messages from CG. cgprsCgAlarmTransSuccess - The GGSN has successfully sent Data Record Transfer Request Message to CG after the failure. cgprsCgAlarmCapacityFull - The GGSN is out of memory and has failed to buffer a G-CDR internally. cgprsCgAlarmCapacityFree - The GGSN is able to buffer G-CDR after the failure to buffer G-CDRs. cgprsCgAlarmEchoFailure - The GGSN has repeatedly failed to receive the Echo Response Messages from the CG for the Echo Request message. cgprsCgAlarmEchoRestored - The GGSN has got the Echo Response from the CG after the cgprsCgAlarmEchoFailure has been detected. cgprsCgAlarmCdrDiscard - The G-CDRs are discarded. cgprsCgAlarmCdrDiscardRestored - This is to indicate that GGSN has started buffering G-CDRs after cgprsCgAlarmCdrDiscard has occured. cgprsCgAlarmChargingDisabled - Indicates that charging transactions on the GGSN are disabled. cgprsCgAlarmChargingEnabled - Indicates that charging transactions on the GGSN are enabled.
cgprsCgGatewayGroupAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgGatewayGroupAlarmHistAddress. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cgprsCgGatewayGroupAlarmHistSeverity	This object indicates the severity of the alarm. Represents the perceived alarm severity associated with a service or safety affecting condition and/or event. These are based on ITU severities, except

	that info(7) is added. cleared(1) - Indicates a previous alarm condition has been cleared. It is not required (unless specifically stated elsewhere on a case by case basis) that an alarm condition that has been cleared will produce a notification or other event containing an alarm severity with this value. indeterminate(2) - Indicates that the severity level cannot be determined. critical(3) - Indicates that a service or safety affecting condition has occurred and an immediate corrective action is required. major(4) - Indicates that a service affecting condition has occurred and an urgent corrective action is required. minor(5) - Indicates the existence of a non-service affecting condition and that corrective action should be taken in order to prevent a more serious (for example, service or safety affecting) condition. warning(6) - Indicates the detection of a potential or impending service or safety affecting condition, before any significant effects have been felt. info(7) - Indicates an alarm condition that does not meet any other severity definition. This can include important, but non-urgent, notices or informational events.
cgprsCgGatewayGroupAlarmHistAddress	This object indicates the IP address that is used to uniquely identify the CG.
cgprsCgGatewayGroupAlarmHistInfo	This object provides detailed information when a GPRS charging gateway or charging related alarm is generated.
cgprsCgGroupIndex	A locally unique identifier for the charging groups on GGSN. Note: There is support for only 30 charging groups (0-29). Where charging group 0 is also referred as default charging gateway group.
cgprsCgGatewayGroupAlarmHistIndex	This object indicates a monotonically increasing integer for the sole purpose of indexing the charging gateway and charging related alarms in a charging group. When the index reaches the maximum value it will wrap around to one.

Go Top

SECTION 13.14

Trap: cgprsCgGatewayGroupAlarmNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ChargingState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The charging transactions on the gateway are disabled.	ChargingState	SPGW
ChargingState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The charging transactions on the gateway are enabled	ChargingState	SPGW

Description:

```
A cgprsCgGroupAlarmNotif signifies that a GPRS related        alarm is detected in the managed system.
This alarm is sent after an entry has been added to
cgprsCgGatewayGroupAlarmHistTable.
```

Default Message:

$NodeDisplayName . The Charging gateway is down
$NodeDisplayName . The charging gateway is up
$NodeDisplayName . The gateway has repeatedly failed to receive responses for the data record transfer request messages from the charging gateway.
$NodeDisplayName -- The gateway has successfully sent data record transfer request messages to the charging gateway.
$NodeDisplayName -- The gateway is out of memory and has failed to buffer a G-CDR internally.
$NodeDisplayName -- The gateway is able to buffer G-CDRs after the failure to buffer G-CDRs.
$NodeDisplayName -- The gateway has repeatedly failed to receive the echo response messages from the charging gateway for the echo request message.
$NodeDisplayName -- The gateway received an echo response from the charging gateway.
$NodeDisplayName -- The gateway has discarded G-CDRs.
$NodeDisplayName -- The gateway has started buffering G-CDRs after G-CDRs have been discarded.
$NodeDisplayName -- The charging transactions on the gateway are disabled.
$NodeDisplayName -- The charging transactions on the gateway are enabled.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cgprsCgGatewayGroupAlarmHistType	This object indicates the type of GPRS, charging gateway or charging related alarm. Identifies the possible types of GPRS charging gateway and charging related alarm. cgprsCgAlarmCgDown - CG is down. cgprsCgAlarmCgUp - CG is up. cgprsCgAlarmTransFailure - The GGSN has repeatedly failed to receive responses for Data Record Transfer Request Messages from CG. cgprsCgAlarmTransSuccess - The GGSN has successfully sent Data Record Transfer Request Message to CG after the failure. cgprsCgAlarmCapacityFull - The GGSN is out of memory and has failed to buffer a G-CDR internally. cgprsCgAlarmCapacityFree - The GGSN is able to buffer G-CDR after the failure to buffer G-CDRs. cgprsCgAlarmEchoFailure - The GGSN has repeatedly failed to receive the Echo Response Messages from the CG for the Echo Request message. cgprsCgAlarmEchoRestored - The GGSN has got the Echo Response from the CG after the cgprsCgAlarmEchoFailure has been detected. cgprsCgAlarmCdrDiscard - The G-CDRs are discarded. cgprsCgAlarmCdrDiscardRestored - This is to indicate that GGSN has started buffering G-CDRs after cgprsCgAlarmCdrDiscard has occured. cgprsCgAlarmChargingDisabled - Indicates that charging transactions on the GGSN are disabled. cgprsCgAlarmChargingEnabled - Indicates that charging transactions on the GGSN are enabled.
cgprsCgGatewayGroupAlarmHistAddrType	This object indicates the type of Internet address given in cgprsCgGatewayGroupAlarmHistAddress. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address

	that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cgprsCgGatewayGroupAlarmHistSeverity	This object indicates the severity of the alarm. Represents the perceived alarm severity associated with a service or safety affecting condition and/or event. These are based on ITU severities, except that info(7) is added. cleared(1) - Indicates a previous alarm condition has been cleared. It is not required (unless specifically stated elsewhere on a case by case basis) that an alarm condition that has been cleared will produce a notification or other event containing an alarm severity with this value. indeterminate(2) - Indicates that the severity level cannot be determined. critical(3) - Indicates that a service or safety affecting condition has occurred and an immediate corrective action is required. major(4) - Indicates that a service affecting condition has occurred and an urgent corrective action is required. minor(5) - Indicates the existence of a non-service affecting condition and that corrective action should be taken in order to prevent a more serious (for example, service or safety affecting) condition. warning(6) - Indicates the detection of a potential or impending service or safety affecting condition, before any significant effects have been felt. info(7) - Indicates an alarm condition that does not meet any other severity definition. This can include important, but non-urgent, notices or informational events.
cgprsCgGatewayGroupAlarmHistAddress	This object indicates the IP address that is used to uniquely identify the CG.
cgprsCgGatewayGroupAlarmHistInfo	This object provides detailed information when a GPRS charging gateway or charging related alarm is generated.

cgprsCgGroupIndex	A locally unique identifier for the charging groups on GGSN. Note: There is support for only 30 charging groups (0-29). Where charging group 0 is also referred as default charging gateway group.
cgprsCgGatewayGroupAlarmHistIndex	This object indicates a monotonically increasing integer for the sole purpose of indexing the charging gateway and charging related alarms in a charging group. When the index reaches the maximum value it will wrap around to one.

Go Top

SECTION 13.15

Trap: ciscoDiaBaseProtPeerConnectionDownNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPeerConnectionState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	SPGW
DiameterPeerConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	SPGW
DiameterPeerConnectionState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The diameter peer $cdbpPeerId state is down.	DiameterPeerConnectionState	SPGW
DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	SPGW
DiameterPeerConnectionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The diameter peer $cdbpPeerId state is up.	DiameterPeerConnectionState	SPGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitConnAck.	DiameterPeerConnectionState	SPGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitICEA.	DiameterPeerConnectionState	SPGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is elect.	DiameterPeerConnectionState	SPGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is waitReturns.	DiameterPeerConnectionState	SPGW
DiameterPeerConnectionState	Poll	Event	Yes	Informational	$NodeDisplayName -- The diameter peer $cdbpPeerId state is closing.	DiameterPeerConnectionState	SPGW

Description:

```
An ciscoDiaBaseProtPeerConnectionDownNotif notification           is sent when both the following conditions are true:
1) the value of
ciscoDiaBaseProtEnablePeerConnectionDownNotif is true(1)
2) cdbpPeerStatsState changes to closed(1).
It can be utilized by an NMS to trigger logical/physical
entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The peer $cdbpPeerId state is down.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpLocalId	The implementation identification string for the Diameter software in use on the system, for example; 'diameterd'
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 13.16

Trap: ciscoDiaBaseProtPermanentFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterPermanentFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol permanent failures for the diameter peer $cdbpPeerId has increased.	DiameterPermanentFailure	SPGW

Description:

```
An ciscoDiaBaseProtPermanentFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnablePermanentFailureNotif
   is true(1)
2) the value of cdbpPeerStatsPermanentFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol permanent failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsPermanentFailures	This object represents the Number of permanent failures returned to peer.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 13.17

Trap: ciscoDiaBaseProtProtocolErrorNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterProtocolError	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol errors returned to the diameter peer $cdbpPeerId has increased.	DiameterProtocolError	SPGW

Description:

```
An ciscoDiaBaseProtProtocolErrorNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableProtocolErrorNotif
   is true(1)
2) the value of cdbpPeerStatsProtocolErrors changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol errors returned to the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router

	that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsProtocolErrors	This object represents the Number of protocol errors returned to peer, but not including redirects.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 13.18

Trap: ciscoDiaBaseProtTransientFailureNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DiameterTransientFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The number of protocol transient failures for the diameter peer $cdbpPeerId has increased.	DiameterTransientFailure	SPGW

Description:

```
An ciscoDiaBaseProtTransientFailureNotif notification           is sent when both the following conditions are true:
1) the value of ciscoDiaBaseProtEnableTransientFailureNotif
   is true(1)
2) the value of cdbpPeerStatsTransientFailures changes.
It can be utilized by an NMS to trigger
logical/physical entity table maintenance polls.
```

Default Message:

$NodeDisplayName -- The number of protocol transient failures for the peer $cdbpPeerId has increased.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cdbpPeerId	The server identifier for the Diameter peer. It must be unique and non-empty.
cdbpPeerStatsTransientFailures	This object represents the transient failure count.
cdbpPeerIndex	A number uniquely identifying each Diameter peer with which the host server communicates. Upon reload, cdbpPeerIndex values may be changed.

Go Top

SECTION 13.19

Trap: cegCongestionClearedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-GW-CongestionState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus.	EPC-GW-CongestionState	SPGW
EPC-GW-CongestionState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus. This gateway is rejecting all new calls.	EPC-GW-CongestionState	SPGW
EPC-GW-CongestionState	Trap	Alarm	Yes	Minor	$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus. This gateway is rejecting low priority calls.	EPC-GW-CongestionState	SPGW
EPC-GW-CongestionState	Poll	Alarm	Yes	Normal	$NodeDisplayName -- The EPC Gateway congestion status is normal.	EPC-GW-CongestionState	SPGW
EPC-GW-CongestionState	Poll	Alarm	Yes	Major	$NodeDisplayName -- The EPC Gateway congestion status is high. This gateway is rejecting all new calls.	EPC-GW-CongestionState	SPGW

EPC-GW-CongestionState	Poll	Alarm	Yes	Minor	$NodeDisplayName -- The EPC Gateway congestion status is low. This gateway is rejecting low priority calls.	EPC-GW-CongestionState	SPGW

Description:

```
The gateway sends this notification, when       the gateway congestion level goes below
cegLowCongestionThreshold value.
This gives an indication that the gateway
has recovered from congestion and it can
accept all calls.
```

Default Message:

$NodeDisplayName -- The EPC Gateway congestion status is $cegCongestionStatus.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegVersion	This object represents the current version of the PGW or SGW software running on the gateway. Display format: : :.
cegCongestionStatus	This object represents the gateway congestion status. INTEGER is unknown
cegCongestionDfpWeight	This object represents the dfp value, which is used to measure the congestion level in the gateway.
cegCongestionLowThreshold	This object represents the low threshold for congestion. Congestion DFP metric considers the current CPU memory usage and number of bearers open. On reaching the low congestion threshold, based on the ARP, high priority calls are accepted and those with a lower priority are rejected. When the gateway congestion level goes below this value, the gateway send cegCongestionClearedNotif notification. This notification would indicate that the gateway has recovered from congestion.

Go Top

SECTION 13.20

Trap: cegqCacMaxPdpExceededNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-MaxPdpExceeded	Trap	Alarm	No	Major	$NodeDisplayName -- The number of pdps on the gateway has reached the user-configured maximum of $cegqCacMaxPdpContext for the CAC policy $cegqCacMaxPdpContext_cegqCacPolicyName.	EPC-QOS-MaxPdpExceeded	SPGW

Description:

```
This notification is sent when the number of pdps on the       gateway has reached the user-configured maximum (or threshold).
```

Default Message:

$NodeDisplayName -- The number of pdps on the gateway has reached the user-configured maximum of $cegqCacMaxPdpContext for the CAC policy $cegqCacMaxPdpContext_cegqCacPolicyName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqCacMaxPdpContext	This object defines maximum number that can be created. If total number of activated pdp exceeds the maximum number, the pdp request will be rejected. Value '0' means there is no limit on pdp creation.
cegqCacPolicyName	This object is the CAC policy name which will be attached to one or more APN's.

Go Top

SECTION 13.21

Trap: cegqCacUpgBRateBearerRejNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-BearerRejected	Trap	Alarm	No	Major	$NodeDisplayName -- The gateway is rejecting bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate	EPC-QOS-BearerRejected	SPGW

Description:

```
This notification is sent when bearers are Rejected/Downgraded       by CAC due to requesting for higher bit rate than
user-configured maximum for a certain QCI class.
```

Default Message:

$NodeDisplayName -- The gateway is rejecting bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqCacQciReject	This object is to specify whether the requested MBR/GBR be downgraded or bearer to be rejected if the requested MBR/GBR exceeds the value set in cegqCacQciBitRateType. 'true' - The request will be rejected if exceeded. 'false' - The requested MBR will be downgraded if exceeded. Represents a boolean value.
cegqCacQciBitRate	This object specifies the MBR/GBR allowed for the QCI defined by cegqCacQci.
cegqCacQci	This object specifies the QCI for which MBR/GBR in uplink/downlink has to be set. When the ratetype is set to guaranteed,QCI1-QCI4 are allowed. When the ratetype is set to maximum,QCI1-QCI9 are allowed.
cegqCacQciBitRateType	This object specifies the type of bit rate applicable for QCI denoted by cegqCacQci.
cegqCacQciDirection	This object specifies the direction of traffic.
cegqCacPolicyName	This object is the CAC policy name which will be attached to one or more APN's.

Go Top

SECTION 13.22

Trap: cegqCacUpgBRateBearerRejNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-BearerDowngraded	Trap	Alarm	No	Minor	$NodeDisplayName -- The gateway is downgrading bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate	EPC-QOS-BearerDowngraded	SPGW

Description:

```
This notification is sent when bearers are Rejected/Downgraded        by CAC due to requesting for higher bit rate than
user-configured maximum for a certain QCI class.
```

Default Message:

$NodeDisplayName -- The gateway is rejecting bearers because they requested a higher bit rate than the user-configured maximum for a certain QCI class. Rate: $cegqCacQciBitRate

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqCacQciReject	This object is to specify whether the requested MBR/GBR be downgraded or bearer to be rejected if the requested MBR/GBR exceeds the value set in cegqCacQciBitRateType. 'true' - The request will be rejected if exceeded. 'false' - The requested MBR will be downgraded if exceeded. Represents a boolean value.
cegqCacQciBitRate	This object specifies the MBR/GBR allowed for the QCI defined by cegqCacQci.
cegqCacQci	This object specifies the QCI for which MBR/GBR in uplink/downlink has to be set. When the ratetype is set to guaranteed,QCI1-QCI4 are allowed. When the ratetype is set to maximum,QCI1-QCI9 are allowed.
cegqCacQciBitRateType	This object specifies the type of bit rate applicable for QCI denoted by cegqCacQci.
cegqCacQciDirection	This object specifies the direction of traffic.
cegqCacPolicyName	This object is the CAC policy name which will be attached to one or more APN's.

Go Top

SECTION 13.23

Trap: cegqQciBWMaxReachedNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
EPC-QOS-MaxBandwidthReached	Trap	Alarm	No	Warning	$NodeDisplayName -- The bandwidth available is fully utilized. No more bearers can be admitted for this QCI class.	EPC-QOS-MaxBandwidthReached	SPGW

Description:

```
This notification is sent when the bandwidth allocated for a       certain QCI class has been fully utilized and no further bearer
can be admitted for this QCI class. The notification is sent
when the bandwidth pool utilization reaches the value in
the object cegqBWPoolQciAbsVal.
```

Default Message:

$NodeDisplayName -- The bandwidth available is fully utilized. No more bearers can be admitted for this QCI class.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cegqBWPoolQciAbsVal	This object denotes the absolute value of bandwidth allocated for the QCI set in cegqBWPoolQci.
cegqBWPoolQciAvailBw	This object denotes the absolute available bandwidth left unused for QCI set in cegqBWPoolQci.
cegqBWPoolQci	This object defines the QCI for which the allocation of bandwidth is needed.
cegqCacBWPoolName	This object is the name of the virtual bandwidth pool which will be attached to the APN.

Go Top

SECTION 13.24

Trap: cIscsiInstSessionFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-InstanceSessionState	Trap	Alarm	No	Warning	$NodeDisplayName - The active session has failed for the remote node - $cIscsiInstLastSsnRmtNodeName.	iSCSI-InstanceSessionState	SPGW

Description:

```
Sent when an active session is failed by either the initiator       or the target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The active session has failed for the remote node $cIscsiInstLastSsnRmtNodeName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiInstSsnFailures	This object counts the number of times a session belonging to this instance has been failed.
cIscsiInstLastSsnFailureType	The counter object in the cIscsiInstSsnErrorStatsTable that was incremented when the last session failure occurred. If the reason for failure is not found in the cIscsiInstSsnErrorStatsTable, the value { 0.0 } is used instead.
cIscsiInstLastSsnRmtNodeName	An octet string describing the name of the remote node from the failed session.

cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.

Go Top

SECTION 13.25

Trap: cIscsiIntrLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-InitiatorLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.	iSCSI-InitiatorLoginStatus	SPGW

Description:

```
Sent when a login is failed by a initiator.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the initiator - $cIscsiIntrLastTgtFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiIntrLastTgtFailureAddrType	The type of Internet Network Address in cIscsiIntrLastTgtFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are

	consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiIntrLoginFailures	This object counts the number of times a login attempt from this local initiator has failed.
cIscsiIntrLastFailureType	The type of the most recent failure of a login attempt from this initiator, represented as the OID of the counter object in cIscsiInitiatorLoginStatsTable for which the relevant instance was incremented. A value of 0.0 indicates a type which is not represented by any of the counters in cIscsiInitiatorLoginStatsTable.
cIscsiIntrLastTgtFailureName	An octet string giving the name of the target that failed the last login attempt.
cIscsiIntrLastTgtFailureAddr	An Internet Network Address giving the host address of the target that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

SECTION 13.26

Trap: cIscsiTgtLoginFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
iSCSI-TargetLoginStatus	Trap	Alarm	No	Warning	$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.	iSCSI-TargetLoginStatus	SPGW

Description:

```
Sent when a login is failed by a target.
The implementation of this trap should not send more than
3 notifications of this type in any 10 second time span.
```

Default Message:

$NodeDisplayName - The last login attempt has been failed by the target - $cIscsiTgtLastIntrFailureName.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cIscsiTgtLastIntrFailureAddrType	The type of Internet Network Address in cIscsiTgtLastIntrFailureAddr. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address which is not in one of the formats defined below.

	ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) A global IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g. InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g. from ipv6(2) to ipv4(1)).
cIscsiTgtLoginFailures	This object counts the number of times a login attempt to this local target has failed.
cIscsiTgtLastFailureType	The type of the most recent failure of a login attempt to this target, represented as the OID of the counter object in cIscsiTargetLoginStatsTable for which the relevant instance was incremented. A value of 0.0 indicates a type which is not represented by any of the counters in cIscsiTargetLoginStatsTable.
cIscsiTgtLastIntrFailureName	An octet string giving the name of the initiator that failed the last login attempt.
cIscsiTgtLastIntrFailureAddr	An Internet Network Address giving the host address of the initiator that failed the last login attempt.
cIscsiInstIndex	An arbitrary integer used to uniquely identify a particular ISCSI instance.
cIscsiNodeIndex	An arbitrary integer used to uniquely identify a particular node within an iSCSI instance present on the local system.

Go Top

SECTION 13.27

Trap: cGgsnSACsgR100StateUpNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
CSGGroupState	Trap	Alarm	Yes	Normal	$NodeDisplayName -- The CSG Group $cGgsnSANotifCsgName: $cGgsnSANotifCsgPort is up.	CSGGroupState	SPGW
CSGGroupState	Trap	Alarm	Yes	Major	$NodeDisplayName -- The CSG Group $cGgsnSANotifCsgName: $cGgsnSANotifCsgPort is down	CSGGroupState	SPGW

Description:

```
This notification is generated when CSG state goes        up. The objects in the varbind list represents -
cGgsnSANotifCsgName: CSG group Name.
cGgsnSANotifCsgRealAddressType: Type of CSG group real
                                 IP address.
cGgsnSANotifCsgRealAddress: Real IP address of the
                               CSG group.
cGgsnSANotifCsgVirtualAddrType: Type of CSG group virtual
                                 IP address.
cGgsnSANotifCsgVirtualAddress: Virtual IP address of the
                                  CSG group.
cGgsnSANotifCsgPort: CSG group port number.
```

Default Message:

$NodeDisplayName -- The CSG Group $ cGgsnSANotifCsgName:$cGgsnSANotifCsgPort is up.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnSANotifCsgRealAddressType	This object indicates the type of IP address, for real address of the CSG group. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cGgsnSANotifCsgVirtualAddrType	This object indicates the type of IP address, for virtual address of the CSG group. A value that represents a type of Internet address. unknown(0) An unknown address type. This value MUST be used if the value of the corresponding InetAddress object is a zero-length string. It may also be used to indicate an IP address that is not in one of the formats defined below. ipv4(1) An IPv4 address as defined by the InetAddressIPv4 textual convention. ipv6(2) An IPv6 address as defined by the InetAddressIPv6 textual convention. ipv4z(3) A non-global IPv4 address including a zone index as defined by the InetAddressIPv4z textual convention. ipv6z(4) A non-global IPv6 address including a zone

	index as defined by the InetAddressIPv6z textual convention. dns(16) A DNS domain name as defined by the InetAddressDNS textual convention. Each definition of a concrete InetAddressType value must be accompanied by a definition of a textual convention for use with that InetAddressType. To support future extensions, the InetAddressType textual convention SHOULD NOT be sub-typed in object type definitions. It MAY be sub-typed in compliance statements in order to require only a subset of these address types for a compliant implementation. Implementations must ensure that InetAddressType objects and any dependent objects (e.g., InetAddress objects) are consistent. An inconsistentValue error must be generated if an attempt to change an InetAddressType object would, for example, lead to an undefined InetAddress value. In particular, InetAddressType/InetAddress pairs must be changed together if the address type changes (e.g., from ipv6(2) to ipv4(1)).
cGgsnSANotifCsgName	This object indicates the CSG group name in cGgsnSACsgEntry.
cGgsnSANotifCsgRealAddress	This object indicates the real IP address of the CSG group.
cGgsnSANotifCsgVirtualAddress	This object indicates the virtual IP address of the CSG group.
cGgsnSANotifCsgPort	This object indicates the port number of the CSG group.

Go Top

SECTION 13.28

Trap: cGgsnExtSubsTraceFailNotif

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
SubscriberTraceFailure	Trap	Alarm	No	Major	$NodeDisplayName -- The activation for the subscriber trace : $cGgsnExtSubscriberTraceId has failed due to $cGgsnExtSubscrTraceFailReason	SubscriberTraceFailure	SPGW

Description:

```
This notification is triggered on failure of a        subscriber trace activation.
```

Default Message:

$NodeDisplayName -- The activation for the subscriber trace : $cGgsnExtSubscriberTraceId has failed due to $cGgsnExtSubscrTraceFailReason.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cGgsnExtSubscriberMcc	MCC value of the subscriber, for which trace activation failure has occured.
cGgsnExtSubscriberMnc	MNC value of the subscriber, for which trace activation failure has occured.
cGgsnExtSubscriberTraceId	Trace Identifier of the subscriber, for which trace activation failure has occured.
cGgsnExtSubscrTraceFailReason	Reason for the trace activation failure.

Go Top

SECTION 13.29

Trap: ciscoTap2MediationTimedOut

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationTimedOut	Trap	Alarm	Yes	Normal	$NodeDisplayName - Tap2Mediation status is active.	Tap2MediationTimedOut	SPGW
Tap2MediationTimedOut	Trap	Alarm	Yes	Critical	$NodeDisplayName - Tap2Mediation status is notInService.	Tap2MediationTimedOut	SPGW
Tap2MediationTimedOut	Trap	Alarm	Yes	Warning	$NodeDisplayName - Tap2Mediation status is notReady.	Tap2MediationTimedOut	SPGW
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndGo.	Tap2MediationTimedOut	SPGW
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is createAndWait.	Tap2MediationTimedOut	SPGW
Tap2MediationTimedOut	Trap	Event	Yes	Informational	$NodeDisplayName - Tap2Mediation status is destroy.	Tap2MediationTimedOut	SPGW

Description:

```
When an intercept is autonomously removed by an intercepting       device, such as due to the time specified in
cTap2MediationTimeout arriving, the device notifies the manager
of the action.
```

Default Message:

$NodeDisplayName - Tap2Mediation status is active.
$NodeDisplayName - Tap2Mediation status is notReady.
$NodeDisplayName - Tap2Mediation status is notInService.
$NodeDisplayName - Tap2Mediation status is createAndGo.
$NodeDisplayName - Tap2Mediation status is createAndWait.
$NodeDisplayName - Tap2Mediation status is destroy.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2MediationStatus	The status of this conceptual row. This object is used to manage creation, modification and deletion of rows in this table. cTap2MediationTimeout may be modified at any time (even while the row is active). But when the row is active, the other writable objects may not be modified without setting its value to 'notInService'. The entry may not be deleted or deactivated by setting its value to 'destroy' or 'notInService' if there is any associated entry in cTap2StreamTable. The RowStatus textual convention is used to manage the creation and deletion of conceptual rows, and is used as the value of the SYNTAX clause for the status column of a conceptual row (as described in Section 7.7.1 of [2].) The status column has six defined values: - `active', which indicates that the conceptual row is available for use by the managed device; - `notInService', which indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device (see NOTE below); - `notReady', which indicates that the conceptual row exists in the agent, but is missing information necessary in order to be available for use by the managed device; - `createAndGo', which is supplied by a management station wishing to create a new instance of a conceptual row and to have its status automatically set to active, making it available for use by the managed device;

- `createAndWait', which is supplied by a management
station wishing to create a new instance of a
conceptual row (but not make it available for use by
the managed device); and,
- `destroy', which is supplied by a management station
wishing to delete all of the instances associated with
an existing conceptual row.

Whereas five of the six values (all except `notReady') may
be specified in a management protocol set operation, only
three values will be returned in response to a management
protocol retrieval operation: `notReady', `notInService' or
`active'. That is, when queried, an existing conceptual row
has only three states: it is either available for use by
the managed device (the status column has value `active');
it is not available for use by the managed device, though
the agent has sufficient information to make it so (the
status column has value `notInService'); or, it is not
available for use by the managed device, and an attempt to
make it so would fail because the agent has insufficient
information (the state column has value `notReady').

NOTE WELL

This textual convention may be used for a MIB table,
irrespective of whether the values of that table's
conceptual rows are able to be modified while it is
active, or whether its conceptual rows must be taken
out of service in order to be modified. That is, it is
the responsibility of the DESCRIPTION clause of the
status column to specify whether the status column must
not be `active' in order for the value of some other
column of the same conceptual row to be modified. If
such a specification is made, affected columns may be
changed by an SNMP set PDU if the RowStatus would not
be equal to `active' either immediately before or after
processing the PDU. In other words, if the PDU also
contained a varbind that would change the RowStatus
value, the column in question may be changed if the
RowStatus was not equal to `active' as the PDU was
received, or if the varbind sets the status to a value
other than 'active'.

Also note that whenever any elements of a row exist, the
RowStatus column must also exist.

To summarize the effect of having a conceptual row with a
status column having a SYNTAX clause value of RowStatus,
consider the following state diagram:

STATE

A	B	C	D
|status col.|status column|			
|status column | is | is |status column			
ACTION |does not exist| notReady | notInService| is active			
set status |noError ->D|inconsist- |inconsistent-|inconsistent-			
column to | or | entValue| Value| Value			
createAndGo |inconsistent- | |			
| Value| |			
set status |noError see 1|inconsist- |inconsistent-|inconsistent-			
column to | or | entValue| Value| Value			
createAndWait |wrongValue | |			
set status |inconsistent- |inconsist- |noError |noError			
column to | Value| entValue| |			
active | | | |			
| | or | |			
| | | |			
| |see 2 ->D| ->D| ->D			
set status |inconsistent- |inconsist- |noError |noError ->C			
column to | Value| entValue| |			
notInService | | | |			
| | or | | or			

	see 3 ->C| ->C|wrongValue	
set status	noError	noError	noError	noError
column to				
destroy	->A	->A	->A	->A
set any other	see 4	noError	noError	see 5
column to some				
value		see 1| ->C| ->D

(1) goto B or C, depending on information available to the agent.
(2) if other variable bindings included in the same PDU, provide values for all columns which are missing but required, then return noError and goto D.
(3) if other variable bindings included in the same PDU, provide values for all columns which are missing but required, then return noError and goto C.
(4) at the discretion of the agent, the return value may be either:
inconsistentName: because the agent does not choose to create such an instance when the corresponding RowStatus instance does not exist, or
inconsistentValue: if the supplied value is inconsistent with the state of some other MIB object's value, or
noError: because the agent chooses to create the instance.
If noError is returned, then the instance of the status column must also be created, and the new state is B or C, depending on the information available to the agent. If inconsistentName or inconsistentValue is returned, the row remains in state A.
(5) depending on the MIB definition for the column/table, either noError or inconsistentValue may be returned.
NOTE: Other processing of the set request may result in a response other than noError being returned, e.g., wrongValue, noCreation, etc.

Conceptual Row Creation

There are four potential interactions when creating a conceptual row: selecting an instance-identifier which is not in use; creating the conceptual row; initializing any objects for which the agent does not supply a default; and, making the conceptual row available for use by the managed device.

Interaction 1: Selecting an Instance-Identifier

The algorithm used to select an instance-identifier varies for each conceptual row. In some cases, the instance-identifier is semantically significant, e.g., the destination address of a route, and a management station selects the instance-identifier according to the semantics.

In other cases, the instance-identifier is used solely to distinguish conceptual rows, and a management station without specific knowledge of the conceptual row might examine the instances present in order to determine an unused instance-identifier. (This approach may be used, but it is often highly sub-optimal; however, it is also a questionable practice for a naive management station to attempt conceptual row creation.)

Alternately, the MIB module which defines the conceptual row might provide one or more objects which provide assistance in determining an unused instance-identifier. For example, if the conceptual row is indexed by an integer-value, then an object having an integer-valued SYNTAX clause might be defined for such a purpose, allowing a management station to issue a management protocol retrieval operation. In order to avoid unnecessary collisions between competing management stations, `adjacent' retrievals of this object should be different.

Finally, the management station could select a pseudo-random

number to use as the index. In the event that this index was already in use and an inconsistentValue was returned in response to the management protocol set operation, the management station should simply select a new pseudo-random number and retry the operation.

A MIB designer should choose between the two latter algorithms based on the size of the table (and therefore the efficiency of each algorithm). For tables in which a large number of entries are expected, it is recommended that a MIB object be defined that returns an acceptable index for creation. For tables with small numbers of entries, it is recommended that the latter pseudo-random index mechanism be used.

Interaction 2: Creating the Conceptual Row

Once an unused instance-identifier has been selected, the management station determines if it wishes to create and activate the conceptual row in one transaction or in a negotiated set of interactions.

Interaction 2a: Creating and Activating the Conceptual Row

The management station must first determine the column requirements, i.e., it must determine those columns for which it must or must not provide values. Depending on the complexity of the table and the management station's knowledge of the agent's capabilities, this determination can be made locally by the management station. Alternately, the management station issues a management protocol get operation to examine all columns in the conceptual row that it wishes to create. In response, for each column, there are three possible outcomes:

- a value is returned, indicating that some other management station has already created this conceptual row. We return to interaction 1.
- the exception `noSuchInstance' is returned, indicating that the agent implements the object-type associated with this column, and that this column in at least one conceptual row would be accessible in the MIB view used by the retrieval were it to exist. For those columns to which the agent provides read-create access, the `noSuchInstance' exception tells the management station that it should supply a value for this column when the conceptual row is to be created.
- the exception `noSuchObject' is returned, indicating that the agent does not implement the object-type associated with this column or that there is no conceptual row for which this column would be accessible in the MIB view used by the retrieval. As such, the management station can not issue any management protocol set operations to create an instance of this column.

Once the column requirements have been determined, a management protocol set operation is accordingly issued. This operation also sets the new instance of the status column to `createAndGo'.

When the agent processes the set operation, it verifies that it has sufficient information to make the conceptual row available for use by the managed device. The information available to the agent is provided by two sources: the management protocol set operation which creates the conceptual row, and, implementation-specific defaults supplied by the agent (note that an agent must provide implementation-specific defaults for at least those objects which it implements as read-only). If there is sufficient information available, then the conceptual row is created, a `noError' response is returned, the status column is set to `active', and no further interactions are necessary (i.e., interactions 3 and 4 are skipped). If there is insufficient information, then the conceptual row is not created, and the set operation fails with an error of `inconsistentValue'.

On this error, the management station can issue a management protocol retrieval operation to determine if this was because it failed to specify a value for a required column,

or, because the selected instance of the status column already existed. In the latter case, we return to interaction 1. In the former case, the management station can re-issue the set operation with the additional information, or begin interaction 2 again using `createAndWait' in order to negotiate creation of the conceptual row.

NOTE WELL

Regardless of the method used to determine the column requirements, it is possible that the management station might deem a column necessary when, in fact, the agent will not allow that particular columnar instance to be created or written. In this case, the management protocol set operation will fail with an error such as `noCreation' or `notWritable'. In this case, the management station decides whether it needs to be able to set a value for that particular columnar instance. If not, the management station re-issues the management protocol set operation, but without setting a value for that particular columnar instance; otherwise, the management station aborts the row creation algorithm.

Interaction 2b: Negotiating the Creation of the Conceptual Row

The management station issues a management protocol set operation which sets the desired instance of the status column to `createAndWait'. If the agent is unwilling to process a request of this sort, the set operation fails with an error of `wrongValue'. (As a consequence, such an agent must be prepared to accept a single management protocol set operation, i.e., interaction 2a above, containing all of the columns indicated by its column requirements.) Otherwise, the conceptual row is created, a `noError' response is returned, and the status column is immediately set to either `notInService' or `notReady', depending on whether it has sufficient information to make the conceptual row available for use by the managed device. If there is sufficient information available, then the status column is set to `notInService'; otherwise, if there is insufficient information, then the status column is set to `notReady'. Regardless, we proceed to interaction 3.

Interaction 3: Initializing non-defaulted Objects

The management station must now determine the column requirements. It issues a management protocol get operation to examine all columns in the created conceptual row. In the response, for each column, there are three possible outcomes:

- a value is returned, indicating that the agent implements the object-type associated with this column and had sufficient information to provide a value. For those columns to which the agent provides read-create access (and for which the agent allows their values to be changed after their creation), a value return tells the management station that it may issue additional management protocol set operations, if it desires, in order to change the value associated with this column.
- the exception `noSuchInstance' is returned, indicating that the agent implements the object-type associated with this column, and that this column in at least one conceptual row would be accessible in the MIB view used by the retrieval were it to exist. However, the agent does not have sufficient information to provide a value, and until a value is provided, the conceptual row may not be made available for use by the managed device. For those columns to which the agent provides read-create access, the `noSuchInstance' exception tells the management station that it must issue additional management protocol set operations, in order to provide a value associated with this column.
- the exception `noSuchObject' is returned, indicating that the agent does not implement the object-type

associated with this column or that there is no
conceptual row for which this column would be
accessible in the MIB view used by the retrieval. As
such, the management station can not issue any
management protocol set operations to create an
instance of this column.
If the value associated with the status column is
`notReady', then the management station must first deal with
all `noSuchInstance' columns, if any. Having done so, the
value of the status column becomes `notInService', and we
proceed to interaction 4.
Interaction 4: Making the Conceptual Row Available
Once the management station is satisfied with the values
associated with the columns of the conceptual row, it issues
a management protocol set operation to set the status column
to `active'. If the agent has sufficient information to
make the conceptual row available for use by the managed
device, the management protocol set operation succeeds (a
`noError' response is returned). Otherwise, the management
protocol set operation fails with an error of
`inconsistentValue'.
NOTE WELL
A conceptual row having a status column with value
`notInService' or `notReady' is unavailable to the
managed device. As such, it is possible for the
managed device to create its own instances during the
time between the management protocol set operation
which sets the status column to `createAndWait' and the
management protocol set operation which sets the status
column to `active'. In this case, when the management
protocol set operation is issued to set the status
column to `active', the values held in the agent
supersede those used by the managed device.
If the management station is prevented from setting the
status column to `active' (e.g., due to management station
or network failure) the conceptual row will be left in the
`notInService' or `notReady' state, consuming resources
indefinitely. The agent must detect conceptual rows that
have been in either state for an abnormally long period of
time and remove them. It is the responsibility of the
DESCRIPTION clause of the status column to indicate what an
abnormally long period of time would be. This period of
time should be long enough to allow for human response time
(including `think time') between the creation of the
conceptual row and the setting of the status to `active'.
In the absense of such information in the DESCRIPTION
clause, it is suggested that this period be approximately 5
minutes in length. This removal action applies not only to
newly-created rows, but also to previously active rows which
are set to, and left in, the notInService state for a
prolonged period exceeding that which is considered normal
for such a conceptual row.
Conceptual Row Suspension
When a conceptual row is `active', the management station
may issue a management protocol set operation which sets the
instance of the status column to `notInService'. If the
agent is unwilling to do so, the set operation fails with an
error of `wrongValue'. Otherwise, the conceptual row is
taken out of service, and a `noError' response is returned.
It is the responsibility of the DESCRIPTION clause of the
status column to indicate under what circumstances the
status column should be taken out of service (e.g., in order
for the value of some other column of the same conceptual
row to be modified).
Conceptual Row Deletion
For deletion of conceptual rows, a management protocol set
operation is issued which sets the instance of the status
column to `destroy'. This request may be made regardless of
the current value of the status column (e.g., it is possible
to delete conceptual rows which are either `notReady',
`notInService' or `active'.) If the operation succeeds,

	then all instances associated with the conceptual row are immediately removed.
cTap2MediationContentId	cTap2MediationContentId is a session identifier, from the intercept application's perspective, and a content identifier from the Mediation Device's perspective. The Mediation Device is responsible for making sure these are unique, although the SNMP RowStatus row creation process will help by not allowing it to create conflicting entries. Before creating a new entry, a value for this variable may be obtained by reading cTap2MediationNewIndex to reduce the probability of a value collision.

Go Top

SECTION 13.30

Trap: ciscoNtpGeneralConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with all NTP servers is lost	NtpConnectionState	SPGW
NtpConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with NTP server has been restored	NtpConnectionState	SPGW

Description:

```
This trap is sent when the device loses connectivity            to all NTP servers.
```

Default Message:

$NodeDisplayName - Connection with all NTP servers is lost.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 13.31

Trap: ciscoNtpHighPriorityConnFailure

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Critical	$NodeDisplayName - Connection with the high priority NTP server is failed	NtpHighPriorityConnectionState	SPGW
NtpHighPriorityConnectionState	Trap	Alarm	Yes	Normal	$NodeDisplayName - Connection with the high priority NTP server is restored	NtpHighPriorityConnectionState	SPGW

Description:

```
A failure to connect with an high priority NTP server           (e.g. a server at the lowest stratum) is detected.
```

Default Message:

$NodeDisplayName - Connection with the high priority NTP server is failed

Message Substitution Variables:

Common	Substitution variables common to all traps.

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpPeersPeerAddress	The IP address of the peer. When creating a new association, a value should be set either for this object or the corresponding instance of cntpPeersPeerName, before the row is made active.
cntpPeersAssocId	An integer value greater than 0 that uniquely identifies a peer with which the local NTP server is associated.

Go Top

SECTION 13.32

Trap: ciscoNtpSrvStatusChange

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
NtpServerStatus	Trap	Alarm	Yes	Indeterminate	$NodeDisplayName - The NTP server status is unknown	NtpServerStatus	SPGW
NtpServerStatus	Trap	Alarm	Yes	Critical	$NodeDisplayName - The NTP server is not running	NtpServerStatus	SPGW
NtpServerStatus	Trap	Alarm	Yes	Warning	$NodeDisplayName - The NTP server is not synchronized to any time source	NtpServerStatus	SPGW
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to its own local clock	NtpServerStatus	SPGW
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a local hardware refclock	NtpServerStatus	SPGW
NtpServerStatus	Trap	Alarm	Yes	Normal	$NodeDisplayName - The NTP server is synchronized to a remote NTP server	NtpServerStatus	SPGW

Description:

```
This notification is generated whenever the value of           cntpSysSrvStatus changes.
```

Default Message:

$NodeDisplayName - The NTP server status is unknown
$NodeDisplayName - The NTP server is not running
$NodeDisplayName - The NTP server is not synchronized to any time source
$NodeDisplayName - The NTP server is synchronized to its own local clock
$NodeDisplayName - The NTP server is synchronized to a local hardware refclock
$NodeDisplayName - The NTP server is synchronized to a remote NTP server

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cntpSysSrvStatus	Current state of the NTP server with values coded as follows: 1: server status is unknown 2: server is not running 3: server is not synchronized to any time source 4: server is synchronized to its own local clock 5: server is synchronized to a local hardware refclock (e.g. GPS) 6: server is synchronized to a remote NTP server INTEGER is unknown

Go Top

SECTION 13.33

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities

GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is above the high threshold of $GGSNHighThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	SPGW
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	SPGW
GTPReceivedMsgsRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of signalling messages received is $GGSNThresholdValue percent of the signalling throughput limit which is below the low threshold of $GGSNLowThreshold percent of the signalling throughput limit.	GTPReceivedMsgsRateThreshold	SPGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts

	created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.

width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 13.34

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is above the high threshold of $GGSNHighThreshold percent of total signalling messages received.	GTPUnexpectedMsgsThreshold	SPGW
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total signalling messages received.	GTPUnexpectedMsgsThreshold	SPGW
GTPUnexpectedMsgsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of unexpected signalling messages received is $GGSNThresholdValue percent of total signalling messages received which is below the low threshold of $GGSNLowThreshold percent of the total signalling messages received.	GTPUnexpectedMsgsThreshold	SPGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This

	alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the

	number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 13.35

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is above the high threshold of $GGSNHighThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	SPGW

GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	SPGW
GPDUBytesSentRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of G-PDU bytes sent is $GGSNThresholdValue percent of the G-PDU bytes sent throughput limit which is below the low threshold of $GGSNLowThreshold percent of the G-PDU bytes sent throughput limit.	GPDUBytesSentRateThreshold	SPGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold

	(recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 13.36

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is above the high threshold of $GGSNHighThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	SPGW
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	SPGW
GPDUBytesReceivedRateThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The rate of G-PDU bytes received is $GGSNThresholdValue percent of the G-PDU bytes received throughput limit which is below the low threshold of $GGSNLowThreshold percent of the G-PDU bytes received throughput limit.	GPDUBytesReceivedRateThreshold	SPGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289">	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold.

style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 13.37

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is above the high threshold of $GGSNHighThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	SPGW
RejectedPDPContextsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	SPGW

RejectedPDPContextsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of rejected PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is below the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	RejectedPDPContextsThreshold	SPGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This

	alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 13.38

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is above the high threshold of $GGSNHighThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	SPGW
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	SPGW
DroppedPDPContextsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of dropped PDP contexts is $GGSNThresholdValue percent of total PDP contexts created which is below the low threshold of $GGSNLowThreshold percent of total PDP contexts created.	DroppedPDPContextsThreshold	SPGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	Alarm Description
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the

Roman";">IPOutboundNoRoutesThreshold	number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 13.39

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ActiveGTPVersion0PDPsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of active GTP version 0 PDP contexts is $GGSNThresholdValue percent of the active GTP version 0 PDP contexts limit which is above the high threshold of $GGSNHighThreshold percent of the active GTP version 0 PDP contexts limit.	ActiveGTPVersion0PDPsThreshold	SPGW
ActiveGTPVersion0PDPsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of active GTP version 0 PDP contexts is $GGSNThresholdValue percent of the active GTP version 0 PDP contexts limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the active GTP version 0 PDP contexts limit.	ActiveGTPVersion0PDPsThreshold	SPGW
ActiveGTPVersion0PDPsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of active GTP version 0 PDP contexts is $GGSNThresholdValue percent of the active GTP version 0 PDP contexts limit which is below the low threshold of $GGSNLowThreshold percent of the active GTP version 0 PDP contexts limit.	ActiveGTPVersion0PDPsThreshold	SPGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	Alarm Description
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

	Substitution variables for Node related data. The Node is

Node	obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 13.40

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ActiveGTPVersion1PDPsThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of active GTP version 1 PDP contexts is $GGSNThresholdValue percent of the active GTP version 1 PDP contexts limit which is above the high threshold of $GGSNHighThreshold percent of the active GTP version 1 PDP contexts limit.	ActiveGTPVersion1PDPsThreshold	SPGW
ActiveGTPVersion1PDPsThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of active GTP version 1 PDP contexts is $GGSNThresholdValue percent of the active GTP version 1 PDP contexts limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the active GTP version 1 PDP contexts limit.	ActiveGTPVersion1PDPsThreshold	SPGW
ActiveGTPVersion1PDPsThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of active GTP version 1 PDP contexts is $GGSNThresholdValue percent of the active GTP version 1 PDP contexts limit which is below the low threshold of $GGSNLowThreshold percent of the active GTP version 1 PDP contexts limit.	ActiveGTPVersion1PDPsThreshold	SPGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	**Alarm Description**
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a

	percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 13.41

Status: Threshold Crossing Alarms for the mobile gateways

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Major	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is above the high threshold of $GGSNHighThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	SPGW
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Warning	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is between the high threshold of $GGSNHighThreshold percent and the low threshold of $GGSNLowThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	SPGW
G-CDRMessagesPendingThreshold	Poll	Alarm	Yes	Normal	$NodeDisplayName - The number of G-CDR messages pending is $GGSNThresholdValue percent of the G-CDR messages pending limit which is below the low threshold of $GGSNLowThreshold percent of the G-CDR messages pending limit.	G-CDRMessagesPendingThreshold	SPGW

Description: Threshold Crossing Alarms for the mobile gateways

Alarm Name	Alarm Description
width="289"> style="font-family: "Times New Roman";">GTPReceivedMsgsRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of signalling messages received as a percentage of the maximum signalling rate exceeds either the high or low threshold. It is cleared when the value is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GTPUnexpectedMsgsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of unexpected signalling messages received as a percentage of total signalling messages received exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesSentRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes sent as a percentage of the G-PDU bytes sent throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">GPDUBytesReceivedRateThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the rate of G-PDU bytes received as a percentage of the G-PDU bytes received throughput limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the rate is below the low threshold.
width="289"> style="font-family: "Times New Roman";">RejectedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of rejected PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">DroppedPDPContextsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of dropped PDP contexts as a percentage of total PDP contexts created exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">ActiveGTPVersion0PDPsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 0 PDP contexts as a percentage of the active GTP version 0 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289">	width="516">

style="font-family: "Times New Roman";">ActiveGTPVersion1PDPsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of active GTP version 1 PDP contexts as a percentage of the active GTP version 1 PDP contexts limit exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">G-CDRMessagesPendingThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of G-CDR messages pending as a percentage of the G-CDR messages pending limit exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPInboundHeaderErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of inbound datagrams with header errors as a percentage of total inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundDiscardsThreshold	style="font-family: "Times New Roman";">This alarm is raised when the number of discarded outbound datagrams as a percentage of outbound datagram requests exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPOutboundNoRoutesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of outbound datagrams discarded because of no route as a percentage of outbound datagram requests exceeds either the high or low threshold. This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPReassemblyFailuresThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP reassembly failures as a percentage of inbound datagrams exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">UDPIncomingErrorsThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of UDP datagrams received in error as a percentage of UDP datagrams delivered exceeds either the high or low threshold. style="font-family: "Times New Roman";">This alarm is cleared when the number is below the low threshold.
width="289"> style="font-family: "Times New Roman";">IPLocalPoolInUseAddressesThreshold	width="516"> style="font-family: "Times New Roman";">This alarm is raised when the number of IP local pool addresses exceeds the rising threshold (recommended 80%) of the total IP addresses available. This alarm is cleared when the number is below the low threshold.

Message Substitution Variables:

Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router

	that sent the trap.
GGSNHighThreshold	The high threshold for gateway TCAs.
GGSNLowThreshold	The low threshold for gateway TCAs.
GGSNThresholdState	Values are High, Medium, or Low
GGSNThresholdValue	The value of the variable measured for this TCA.

Operational Information:

Go Top

SECTION 13.42

Trap: ciscoTap2MIBActive

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MIBActive	Trap	Event	No	Informational	$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.	Tap2MIBActive	SPGW

Description:

```
This Notification is sent when an intercepting router or        switch is first capable of intercepting a packet corresponding
to a configured data stream. The value of the corresponding
cTap2StreamType which identifies the actual intercept stream
type is included in this notification.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.  Filter
installation can take a long period of time, during which call
progress may be delayed.
```

Default Message:

$NodeDisplayName - Is capable of intercepting a packet corresponding to a configured " $cTap2StreamType " stream.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 13.43

Trap: ciscoTap2MediationDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2MediationDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .	Tap2MediationDebug	SPGW

Description:

```
When there is intervention needed due to some events related       to entries configured in cTap2MediationTable, the device
notifies the manager of the event.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.
```

Default Message:

$NodeDisplayName - cTap2MediationTable is reconfigured with following values DebugMediationId $cTap2DebugMediationId , cap2DebugMessage :- $cTap2DebugMessage .

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 13.44

Trap: ciscoTap2StreamDebug

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2StreamDebug	Trap	Event	No	Informational	$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId	Tap2StreamDebug	SPGW

Description:

```
When there is intervention needed due to some events related        to entries configured in cTap2StreamTable, the device
notifies the manager of the event.
This notification may be generated in conjunction with the
intercept application, which is designed to expect the
notification to be sent as reliably as possible, e.g., through
the use of a finite number of retransmissions until
acknowledged, as and when such mechanisms are available; for
example, with SNMPv3, this would be an InformRequest.
```

Default Message:

$NodeDisplayName - cTap2StreamTable is reconfigured with following values DebugMediationId : $cTap2DebugMediationId :- $cTap2DebugMessage with DebugStreamid : $cTap2DebugStreamId.br>

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.
cTap2DebugMediationId	The value of this object is that of cTap2MediationContentId identifying an entry in cTap2MediationTable. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2MediationTable fails and this debug message conveys more detailed information regarding the failure.
cTap2DebugStreamId	The value of this object is that of cTap2StreamIndex of an entry in cTap2StreamTable. This object along with cTap2DebugMediationId identifies an entry in cTap2StreamTable.

	The value of this object may be zero, in which this debug message is regarding a Mediation Device, but not a particular stream. Note this object may contain a value for which an entry in cTap2MediationTable does not exist. This happens when creation of an entry in cTap2StreamTable fails.
cTap2DebugMessage	A text string contains the debug message.
cTap2DebugIndex	Index to the debug table.

Go Top

SECTION 13.45

Trap: ciscoTap2Switchover

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
Tap2Switchover	Trap	Event	No	Informational	$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.	Tap2Switchover	SPGW

Description:

```
This notification is sent when there is a redundant (standby)        route processor available on the intercepting device and the
current active processor is going down causing standby to
takeover. Note that this notification may be sent by the
intercepting device only when it had a chance to know before it
goes down.
Mediation device when received this notification should assume
that configured intercepts on the intercepting device no longer
exist, when the standby processor takes control. This means that
the Mediation device should again configure the intercepts.
```

Default Message:

$NodeDisplayName - Redundant (standby) route processor is available on the intercepting device and the current active processor is going down causing standby to takeover.

Message Substitution Variables:

Common	Substitution variables common to all traps.
Node	Substitution variables for Node related data. The Node is obtained from the MWTM database based on the IP address of the router that sent the trap.

Go Top

SECTION 13.46

Status: ApnInstanceStateAdded and ApnInstanceStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceState	Poll	Event	No	Normal	APN $ApnDisplayName on gateway $NodeDisplayName added in state Active/ActiveReason.	ApnInstanceState	SPGW
ApnInstanceState	Poll	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName added in state $ApnInstanceState/$ApnInstanceStateReason.	ApnInstanceState	SPGW
ApnInstanceState	Poll	Event	No	Normal	APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to Active/ActiveReason.	ApnInstanceState	SPGW
ApnInstanceState	Poll	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to $ApnInstanceState/$ApnInstanceStateReason.	ApnInstanceState	SPGW

Description:

The ApnInstanceStateAdded and ApnInstanceStateChanged status eventsprovide information when an ApnInstance object is added to the MWTM object model or when MWTM detects that the state of an ApnInstance has

changed. An ApnInstance is defined as an access-point and accesspoint-name defined on a gateway router. An ApnInstance object is located under the gateway Node object in the MWTM object tree. The value of ApnInstanceState indicates the new state. Possible values of ApnInstanceState include:

- Active - Traffic may flow over this ApnInstance.
- Unknown - The attempt to determine the state of the ApnInstance failed.
- Warning - The ApnInstance is Active however some underlying status contributor of this ApnInstance is not fully functional.
- Deleted - The ApnInstance has been deleted from the object database.

Default Message:

- APN $ApnDisplayName on gateway $NodeDisplayName added in state $ApnInstanceState/$ApnInstanceStateReason.
- APN $ApnDisplayName on gateway $NodeDisplayName changed state from $ApnInstanceLastState to $ApnInstanceState/$ApnInstanceStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
ApnInstanceState	The current state of the ApnInstance.
ApnInstanceStateReason	The current state reason of of the ApnInstance.
ApnInstanceLastState	The previous state of the ApnInstance.

Operational Information:

See also:

Go Top

SECTION 13.47

Status: ApnStateAdded and ApnStateChanged

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnState	Poll	Event	No	Normal	APN $ApnDisplayName added in state Active/ActiveReason.	ApnState	SPGW
ApnState	Poll	Event	No	Informational	APN $ApnDisplayName added in state $ApnState/$ApnStateReason.	ApnState	SPGW
ApnState	Poll	Event	No	Normal	APN $ApnDisplayName changed state from $ApnLastState to Active/ActiveReason.	ApnState	SPGW
ApnState	Poll	Event	No	Informational	APN $ApnDisplayName changed state from $ApnLastState to $ApnState/$ApnStateReason.	ApnState	SPGW

Description:

The ApnStateAdded and ApnStateChanged status events provideinformation when an Apn object is added to the MWTM object model or when MWTM detects that the state of an Apn has changed. An Apn is defined as an aggregation of a set of ApnInstance objects defined across a set of gateway routers. An Apn object is located as a top level object in the MWTM object tree. The value of ApnState indicates the new state. Possible values of ApnState include:

- Active - Traffic may flow over this Apn.
- Warning - The Apn is Active however one or more of its constituent ApnInstances is not fully functional.
- Deleted - The Apn has been deleted from the object database.

Default Message:

- Apn $ApnDisplayName added in state $ApnState/$ApnStateReason.
- Apn $ApnDisplayName changed state from $ApnLastState to $ApnState/$ApnStateReason.

Message Substitution Variables:

Node	Substitution variables for Node related data.
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
ApnState	The current state of the Apn.
ApnStateReason	The current state reason of of the Apn.
ApnLastState	The previous state of the Apn.

Operational Information:

See also:

Go Top

SECTION 13.48

UserAction: ApnInstanceIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceIgnoredSet	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.	ApnInstanceIgnoredSet	SPGW

Description:

The ApnInstanceIgnoredSet UserAction event provides information when a ApnInstance's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the ApnInstance in the aggregation algorithm in determining the state of a Node or Apn. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The ApnInstance is to be excluded from state aggregation.
- False - The ApnInstance is to be included in state aggregation.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node	
Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
ApnInstanceState	The current state of the ApnInstance.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the ApnInstances which are currently ignored select the ApnInstance folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 13.49

UserAction: ApnIgnoredSet

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnIgnoredSet	User Action	Event	No	Informational	APN $ApnDisplayName ignore flag is set to $IgnoredFlag by $User.	ApnIgnoredSet	SPGW

Description:

The ApnIgnoredSet UserAction event provides information when a Apn's Ignore flag is set by a user. The Ignore flag indicates to MWTM whether or not to include the Apn in the aggregation algorithm in determining the state of higher level objects. The value of IgnoredFlag
indicates the new ignore state. Possible values of IgnoredFlag include:

- True - The Apn is to be excluded from state aggregation.
- False - The Apn is to be included in state aggregation.

Default Message:

APN $ApnDisplayName ignore flag is set to $IgnoredFlag by $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
ApnState	The current state of the Apn.
IgnoredFlag	The current state of the Ignore flag.
User	The user who requested the ignore flag to be set.

Operational Information:

- The setting of the ignore flag to True can lead to confusing aggregated states. To find the Apns which are currently ignored select the Apn folder in the MWTM Main window and sort on the Ignored field.

Go Top

SECTION 13.50

UserAction: ApnInstanceUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceUserDataUpdated	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName edited by user $User.	ApnInstanceUserDataUpdated	SPGW

Description:

The ApnInstanceUserDataUpdated UserAction event provides information when a ApnInstance object's user data has been updated by a MWTM user.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName edited by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.

ApnIndex	The index of the ApnInstance.
User	The user who requested the ApnInstance's data be updated.

Operational Information:

The fields that can be updated for a ApnInstance include:

- The ApnInstance's notes data used for communicating installation dependent information about a ApnInstance.

Go Top

SECTION 13.51

UserAction: ApnUserDataUpdated

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnUserDataUpdated	User Action	Event	No	Informational	APN $ApnDisplayName edited by user $User.	ApnUserDataUpdated	SPGW

Description:

The ApnUserDataUpdated UserAction event provides information when a Apn object's user data has been updated by a MWTM user.

Default Message:

APN $ApnDisplayName edited by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.

ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
User	The user who requested the Apn's data be updated.

Operational Information:

The fields that can be updated for a Apn include:

- The Apn's notes data used for communicating installation dependent information about a Apn.

Go Top

SECTION 13.52

UserAction: ApnInstanceDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnInstanceDeleted	User Action	Event	No	Informational	APN $ApnDisplayName on gateway $NodeDisplayName deleted by user $User.	ApnInstanceDeleted	SPGW

Description:

The ApnInstanceDeleted UserAction event provides information when a ApnInstanceobject's deletion from the MWTM object model database is requested.

Default Message:

APN $ApnDisplayName on gateway $NodeDisplayName deleted by user $User.

Message Substitution Variables:

Node

Substitution variables for Node related data.	
ApnDisplayName	The display name of the ApnInstance.
ApnName	The name of the ApnInstance.
ApnIndex	The index of the ApnInstance.
User	The user who requested the ApnInstance's data be deleted.

Operational Information:

- The deletion of a ApnInstance can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top

SECTION 13.53

UserAction: ApnDeleted

Name	Source	Type	Auto Clear	Severity	Message Text	Correlation Key	Personalities
ApnDeleted	User Action	Event	No	Informational	APN $ApnDisplayName deleted by user $User.	ApnDeleted	SPGW

Description:

The ApnDeleted UserAction event provides information when a Apnobject's deletion from the MWTM object model database is requested.

Default Message:

APN $ApnDisplayName deleted by user $User.

Message Substitution Variables:

Node	
Substitution variables for Node related data.	
ApnDisplayName	The display name of the Apn.
ApnName	The name of the Apn.
ApnIndex	The index of the Apn.
User	The user who requested the Apn's data be deleted.

Operational Information:

- The deletion of a Apn can be requested by the MWTM server itself in some instances during the discovery process. In this case the User variable reflects the userid of the MWTM server.

Go Top
