

## GSRIPC Messages

The following are Internet router interprocess communication (IPC) service routines error messages.

### Error Message

```
%GSRIPC-3-PORT: port ([chars]) already exists
```

**Explanation** The port to be created already exists.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

### Error Message

```
%GSRIPC-3-REXEC: [chars]
```

**Explanation** The remote execution open port has failed.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

### Error Message

```
%GSRIPC-3-SYSCALL: For port ([chars]): [chars] fails (cause: [chars])
```

**Explanation** The IPC kernel system call has failed.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## GT64010 Messages

The following are GT64010 DMA controller driver error messages.

### Error Message

```
%GT64010-3-DMA: Interrupt error, c=[hex], m=[hex], rc=[hex]
```

**Explanation** An unexpected interrupt has been registered from a DMA engine that was not initialized by the software.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%GT64010-1-DMASTALL: DMA interrupt stalled, restarted engine [dec]

**Explanation** The driver timed out while waiting for completion of a DMA task. The DMA engine has been restarted.

**Recommended Action** If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%GT64010-3-NOCHANNEL: Referencing unused DMA channel [dec]

**Explanation** An access to an uninitialized DMA engine has been attempted.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%GT64010-3-TIMER: Interrupt error, c=[hex], m=[hex], rc=[hex]

**Explanation** An unexpected timer interrupt was received from a timer element that had not been initialized by the software.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%GT64010-3-TIMERINSTALL: Attempt to install already installed timer [dec]

**Explanation** An attempt was made to initialize a timer element that is already in use.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## GTP Messages

The following are General Packet Radio Service (GPRS) Tunnel Protocol error messages.

### Error Message

```
%GTP-2-GSNSERVICEUPDOWN: GSN service [chars] changed state to [chars]
```

**Explanation** The SGSN service has started or has been shutdown.

**Recommended Action** If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

### Error Message

```
%GTP-2-PDPACTIVATIONFAIL: GTP PDP activation/update failed, GSN: [IP_address],  
TID: [hex][hex], Reason: [chars]
```

**Explanation** A PDP context activation has failed.

**Recommended Action** If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## HAWKEYE Messages

The following are Token Ring protocol control information (PCI) port adapter error messages.

### Error Message

```
%HAWKEYE-3-ADPCHK: Interface [chars], adapter check error
```

**Explanation** The Token Ring interface has encountered an unrecoverable error condition while it was operating and connected to the ring. The interface will automatically shut itself down.

**Recommended Action** Issue the **clear interface token** command to restart the interface. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HAWKEYE-1-DISCOVER: Only found [dec] interfaces on bay [dec], shutting down bay

**Explanation** The Token Ring device driver was unable to communicate with all of the interfaces expected to be on the port adapter module. This condition could indicate that one or more of the interfaces is not functioning. This message may occur during Cisco IOS software initialization or after an OIR of a Token Ring port adapter or module.

**Recommended Action** Reseat the port adapter or module in the slot. If necessary, install it in another slot. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HAWKEYE-3-INITFAIL: [chars] failed to initialize - [chars]

**Explanation** The Token Ring interface has encountered an error while attempting to open a connection to the ring. The specific error that occurred is described in the last half of the error message as one of the following:

- microcode checksum failed—The MAC microcode is corrupted inside the local memory of the interface.
- failed to build receive descriptor ring—There was not enough system memory available to allocate receive buffers for packets.
- init failed — The interface hardware has rejected the request from the device driver request to configure and open the interface.

**Recommended Action** Reset the interface using the clear interface token command in EXEC mode. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HAWKEYE-3-MAC\_CMD\_Q\_OVERFLOW: HAWKEYE ([dec]/[dec]), MAC command queue overflow

**Explanation** The command queue of the specified interface was full when the device driver attempted to send a command to the interface hardware. This condition may occur if the device driver software sends commands faster than the interface hardware can process them. This condition is usually not a critical error, and the interface should continue to function normally. However, if the error message appears repeatedly, it may indicate a more serious problem.

**Recommended Action** If this error appears repeatedly, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information. Otherwise, no action is required.

**Error Message**

%HAWKEYE-1-NOPCIMEMORY: PCI memory unavailable for [chars]

**Explanation** The device driver for the specified interface was unable to allocate the necessary amount of shared memory between the driver and the interface hardware. This condition can occur if the system contains less than the recommended minimum amount of SRAM for the current interface combination. Since shared memory blocks are required for the interface to function, the specified interface will be inoperable until the memory shortage is corrected.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HAWKEYE-1-OLDREV: HAWKEYE(bay [dec]), Port adapter requires Rev 2 CPU, shutting down bay

**Explanation** The device driver has detected an NPE150 CPU version earlier than Revision 2. The Token Ring device driver requires capabilities of an NPE150 Revision 2 or later CPU. This message is specific to Cisco 7200 series routers.

**Recommended Action** Upgrade the Cisco 7200 router processor to an NPE150 Revision 2 or later.

## HD Messages

The following are HD64570 serial controller error messages.

**Error Message**

%HD-1-BADLOOPCABLE: Loopback not supported for a 4T DTE/X.21, port [dec] in slot [dec]

**Explanation** Loopback mode is not allowed when using an X.21 DTE cable on a Quad serial NIM port.

**Recommended Action** Do not enable loopback mode, or use a different cable type.

**Error Message**

%HD-1-BADPORTADAPTER: 4T Port Adapter fault on port [dec] in slot [dec]

**Explanation** A hardware or software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HD-1-BADRING: Bad [chars] ring size

**Explanation** An internal software error has occurred.

**Recommended Action** If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HD-5-LINEFLAP: Unit [dec] excessive modem control changes

**Explanation** Too many modem control interrupts have been received. The port was disabled to prevent excessive use of the CPU.

**Recommended Action** Check the cable on the serial port.

## HDV Messages

The following are High Density Voice (HDV) error messages.

**Error Message**

%HDV-3-DISCOVER: HDV in slot [dec]: the HDV failed to initialize properly.

**Explanation** An initialization action has failed for the HDV. This failure can be caused by a lack of system resources, a missing VIC, an improper VIC installed in the port module, or defective HDV hardware.

**Recommended Action** Power down the router. Check that a supported VIC is properly installed in the HDV port module. Reinsert the VIC, and then reinsert the port module and reboot the router. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HDV-2-FATAL\_ERROR: HDV in slot [dec]: An unrecoverable error occurred.

**Explanation** The HDV card has experienced an internal unrecoverable error. This error may be caused by an internal firmware error or defective HDV hardware.

**Recommended Action** Power down, reinsert the network module, and reboot the router. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HDV-3-FW\_START: HDV in slot [dec]: the firmware on the port module did start properly.

**Explanation** The firmware on the card did not start after a reset. This condition is usually caused by a defective HDV module or improperly seated HDV module.

**Recommended Action** Power down, reinsert the HDV port module, and reboot the router. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HDV-3-HW\_START: HDV in slot [dec]: the port module did not reset and start up properly.

**Explanation** The hardware on the card did not start after a reset. This condition is usually caused by a defective HDV module or improperly seated HDV module.

**Recommended Action** Power down, reinsert the HDV port module, and reboot the router. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HDV-3-INCORRECT\_P MID: HDV in slot [dec]: Incorrect [dec] PM-ID device not supported.

**Explanation** An interface controller device did not have the correct port module ID.

**Recommended Action** Ensure that the HDV port module is inserted properly. If necessary, power down the router and reinsert the HDV port module. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HDV-3-INVALID\_PCI\_ID: HDV in slot [dec]: reports an invalid device id of [hex].

**Explanation** The HDV port module hardware may be defective or improperly seated.

**Recommended Action** Power down, reinsert the network module, and reboot the router. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HDV-1-NO\_DAUGHTER\_CARD: HDV in slot [dec]: no VIC card is inserted in the HDV.

**Explanation** The software did not detect the presence of a VIC inserted in the HDV port module.

**Recommended Action** Check that there is a VIC inserted properly into the HDV. If the VIC is inserted properly, check the part number on the VIC to see if it is supported by the version of Cisco IOS software that running on the router. For further assistance, contact your Cisco technical support representative.

**Error Message**

%HDV-1-NOPCIMEMORY: HDV in slot [dec]: No PCI memory available.

**Explanation** The system has exhausted its memory in the PCI or packet memory. This condition is probably due to heavy traffic congestion but could also indicate a software error.

**Recommended Action** Review the system configuration for performance bottlenecks. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HDV-1-TOOBIG: HDV in slot [dec]: packet size ([dec]) too big.

**Explanation** A packet greater than the 256-byte maximum has been received on this interface.

**Recommended Action** The system should recover. No action is required. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HDV-1-UNKNOWN\_VIC: HDV in slot [dec]: VIC daughter card has an unknown id of [hex]

**Explanation** The software did not recognize the type of VIC that is plugged into the HDV port module.

**Recommended Action** Check the part number on the VIC to see if it is supported in the version of Cisco IOS software running on the router. For further assistance, contact your Cisco technical support representative.

**Error Message**

%HDV-1-UNSUPPORTED\_VIC: HDV in slot [dec]: VIC daughter card ([chars]/[hex]) is unsupported

**Explanation** The type of VIC that is plugged into the HDV is not supported.

**Recommended Action** Replace the VIC in the specified HDV slot with a type that is supported by the version of Cisco IOS software that is running on the router, or change the version of Cisco IOS software to support this type of VIC.

# HDX Messages

The following are error messages related to half-duplex (HDX) finite state machines (FSM).

## Error Message

```
%HDX-3-BADFSM: On int [dec]/[dec], unexpected state [dec], event [dec]
```

**Explanation** An invalid state or event pair has been detected in the Rx and Tx half-duplex state machine.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

# HEARTBEAT Messages

The following are “Heartbeat” error messages.

## Error Message

```
%HEARTBEAT-6-NOT_HEARD: Heartbeat messages have not been heard for [dec] seconds
```

**Explanation** Heartbeat messages have not been received for the time specified in the error message. If heartbeat messages are not received soon, a timeout, which will reset the system, is likely to occur.

**Recommended Action** No action is required.

## Error Message

```
%HEARTBEAT-2-NOT_RUNNING: Heartbeat messages have not been sent for [dec] seconds  
[[chars]] [[chars] [time-stamp]] [[chars] [time-stamp]] [[chars] [time-stamp]]
```

**Explanation** Heartbeat messages have not been sent for the time specified in the error message. If heartbeat messages are not sent soon, a timeout, which will reset the system, is likely to occur.

**Recommended Action** No action is required.

## Error Message

```
%HEARTBEAT-3-TIMED_OUT: Heartbeat messages have failed, resetting system
```

**Explanation** Heartbeat messages have failed, and the system is no longer operational.

**Recommended Action** No action is required.

# HMM\_ASYNC Messages

The following are hex modem network module asynchronous driver error messages.

## Error Message

%HMM\_ASYNC-3-CARD\_FAILED\_DOWNLOAD: Unable to download firmware image to digital modem card in slot [dec].

**Explanation** An attempt to bring up the processor on the digital modem card has failed.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## Error Message

%HMM\_ASYNC-3-HMM\_HARDWARE\_EXCEPTION: HMM: Digital Modem Card [dec] hardware exception : [chars]

**Explanation** An intermittent or permanent hardware failure may have occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## Error Message

%HMM\_ASYNC-3-MODEM\_FAILED\_DIAGS: Digital modem [dec]/[dec] on Simm [dec] failed power on diagnostics.

**Explanation** The digital modem has failed to pass power on diagnostics and will not be used.

**Recommended Action** If the remaining SIMMs passed the diagnostics, remove or replace the defective SIMM before continuing. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## Error Message

%HMM\_ASYNC-3-MODEM\_MAILBOX\_IS\_FULL: HMM Modem [dec]/[dec] Mailbox is Full, command [hex] not sent.

**Explanation** An error has occurred during an attempt to deliver commands to the modem module. This failure may be temporary. If this message repeats every 30 seconds, it may indicate a failed modem module.

**Recommended Action** If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-3-MODEM\_STOPPED\_PROCESSING\_MAIL: HMM Modem [dec]/[dec] failed to accept a new command.

**Explanation** The modem has failed to accept a new command. This failure may be temporary, or the modem may remain unusable until a system reset has been performed.

**Recommended Action** Reset the modem by issuing the **clear modem** command. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-3-NOMEMORY: No memory for [chars] of unit [dec]

**Explanation** The router does not have enough memory to perform the requested function.

**Recommended Action** Consider adding more shared memory. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-4-NO\_MODEMS\_PRESENT: HMM Digital Modem Card [dec] contains no active modems.

**Explanation** There are no modems installed on the network module.

**Recommended Action** Ensure that the network module contains properly installed MICA-6DM SIMMs.

**Error Message**

%HMM\_ASYNC-3-NORAWRXPOOL: Unable to create pool for [dec] raw Rx mode buffers

**Explanation** The router does not have enough I/O memory for the buffers.

**Recommended Action** Consider adding more shared memory. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-3-NORAWTXPOOL: Unable to create pool [dec] raw Tx mode buffers

**Explanation** The router does not have enough I/O memory for the buffers.

**Recommended Action** Consider adding more shared memory. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-3-NOTTYCREATE: Unable to create TTY structure for line [dec]

**Explanation** The system was unable to create a tty line control block for the specified line. This condition may have occurred because there is not enough memory in the router.

**Recommended Action** Consider adding more shared memory. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-3-SIMM\_FAILED\_DOWNLOAD: Unable to download modem firmware image to Simm [dec] in slot [dec].

**Explanation** The modem firmware has failed to load into the SIMM.

**Recommended Action** If the firmware has successfully loaded into remaining SIMMs, remove or replace the defective SIMM before continuing. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-3-SIMM\_RUNTIME\_ERROR: Simm [dec] in slot [dec] has halted due to a Runtime Error.

**Explanation** The portware running on the SIMM was halted because of a runtime error. The six modems contained on the SIMM have been marked “bad” and are no longer usable until the system is reloaded.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log along with the output of the **show modem** and **show modem log** commands, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-3-TDM\_SYNTHESIS\_ERROR: HMM Digital Modem Card [dec] experienced a TDM Synthesis Error.

**Explanation** The digital modem card has failed to send or receive PCM data in time to avoid data loss. This condition may cause the modems to speed shift, retrain, or hang up.

**Recommended Action** Verify that the DS1 interfaces share a common clock source. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-3-UNKNOWN\_MESSAGE: Received unknown message [hex] at mail offset [dec] from modem [dec]/[dec].

**Explanation** An unidentified message has been received from the modem. This condition is a symptom of running an incompatible version of modem firmware.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HMM\_ASYNC-3-UNKNOWNPLATFORM: Unknown Platform type to support HMM Network Module

**Explanation** The network module is not compatible with the current platform into which it is plugged.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## HOOD Messages

The following are LAN controller 100VG-AnyLAN interface error messages.

**Error Message**

%HOOD-3-BADUNIT: Bad unit number [dec]

**Explanation** An internal software error has occurred.

**Recommended Action** If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HOOD-5-CABLEERR: Unit [dec], HP100VG, cable error. Training failed

**Explanation** A 100VG cable or hub is faulty.

**Recommended Action** If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HOOD-5-COLL: Unit [dec], excessive collisions

**Explanation** An Ethernet cable is broken or unterminated, or the transceiver is unplugged.

**Recommended Action** If the transceiver appears to be properly terminated, repair or replace the router.

**Error Message**

%HOOD-5-LOSTCARR: Unit [dec], lost carrier. Transceiver problem?

**Explanation** An Ethernet transceiver is unplugged or defective.

**Recommended Action** Repair or replace the controller.

**Error Message**

%HOOD-5-NOCABLE: Unit [dec], HP100VG, no tone detected. Check cable, hub

**Explanation** A 100VG cable is defective.

**Recommended Action** If this message recurs and either the cable or the hub appears to function, repair or replace the router module.

## HP100VG Messages

The following are 100VG-AnyLAN port adapter driver error messages.

**Error Message**

%HP100VG-1-ACCESS: [chars] access to network denied

**Explanation** Access to the network is denied because of an incompatible configuration.

**Recommended Action** Check the configuration of the hub for Frame Format, Promiscuous, and Repeater bit to indicate proper configuration.

**Error Message**

%HP100VG-5-CABLEERR: [chars] training failed

**Explanation** A 100VG cable or hub is faulty.

**Recommended Action** Repair or replace the cable or hub. If either the cable or the hub appear to function, repair or replace the VG PA interface module.

**Error Message**

%HP100VG-1-DISCOVER: Only found [dec] interfaces on bay [dec], shutting down bay

**Explanation** No VG interface was detected.

**Recommended Action** Ensure that the 100VG PA is properly seated in the slot. Otherwise, repair or replace the 100VG PA interface module.

**Error Message**

%HP100VG-1-DUPMAC: On [chars] LAN segment

**Explanation** Two VG devices on the same LAN segment have the same MAC address.

**Recommended Action** Check the router configuration to ensure that no duplicate MAC address is configured.

**Error Message**

%HP100VG-1-LANCNF: [chars] configuration not compatible with the network

**Explanation** The configuration of the router module is not compatible with the network.

**Recommended Action** Check the configuration of the hub for Frame Format, Promiscuous, and Repeater bit to indicate proper configuration.

**Error Message**

%HP100VG-5-LOSTCARR: [chars] cable/hub problem?

**Explanation** The VG controller has detected that a link to the hub is down because of a cable, hub or VG controller problem.

**Recommended Action** Repair or replace the cable or hub. If either the cable or the hub appear to be functioning, repair or replace the VG PA interface module.

**Error Message**

%HP100VG-5-NOCABLE: [chars] cable fault; tone not detected

**Explanation** A 100VG cable is faulty.

**Recommended Action** Repair or replace the cable. If the cable appears to be functioning, repair or replace the VG PA interface module.

**Error Message**

%HP100VG-3-NOCAM: [chars] hardware CAM device not found

**Explanation** The hardware CAM could not be found on the PA module.

**Recommended Action** Repair or replace the 100VG PA interface module.

**Error Message**

%HP100VG-3-NOTHP100VG: Bay [dec] device ID seen as [hex], expected [hex]

**Explanation** The 100VG PCI device could not be found.

**Recommended Action** Ensure that the 100VG PA device is properly seated in the slot. Otherwise, repair or replace the 100VG PA interface module.

**Error Message**

%HP100VG-3-OWNERR: [chars] packet buffer, pak=[hex]

**Explanation** A software or hardware error has occurred. The HP100VG driver detected that the buffer ring is in an inconsistent and unrecoverable state.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HP100VG-1-TRAINFAIL: [chars] unable to login to the hub

**Explanation** An attempt to log in to the hub has failed.

**Recommended Action** Take action based on the error messages that follow this message.

## HTSP Messages

The following are analog voice hardware adaptation layer software error messages.

**Error Message**

%HTSP-3-CAPABILITYMISMATCH: voice port [chars]: call connection id [[hex] [hex] [hex] [hex]]

**Explanation** The capabilities between the two call legs did not match. The capabilities are negotiated between call legs for codec, VAD, and fax rates.

**Recommended Action** Check that the dial peer configuration is appropriate for the interface in question. Also check that the configuration on the interface is correct.

**Error Message**

%HTSP-3-DSPALARM: voice port [chars]: status=[hex] message=[hex] text=[chars]

**Explanation** The DSP has reported a fatal error. All calls on the DSP were dropped, and a DSP reload was attempted.

**Recommended Action** Verify that the DSP reloaded properly by attempting to place a call on the specified voice port. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HTSP-3-NOEVENT: no free event structure available from [chars] for DSP message

**Explanation** No event structures were remaining in the system pools to alert the router of a voice or signaling event.

**Recommended Action** Check that the voice port for which the event was reported is still operational. If it is not still operational, clear the voice port.

**Error Message**

%HTSP-3-TRUNKNOTSUPPORTED: voice port [chars]: Ground Start trunking not supported

**Explanation** The specified voice port does not support the **connection trunk** command when ground start signaling is configured. Trunking mode on this voice is supported when loop-start signaling is used.

**Recommended Action** Shut down the voice port, remove the **connection trunk** or **signal ground-start** command from the voice port configuration, and restart (unshut) the voice port.

**Error Message**

%HTSP-5-UPDOWN: Trunk port(channel) [[chars]] is [chars]

**Explanation** The trunk port:channel has changed state.

**Recommended Action** No action is required.

## HUB Messages

The following are Cisco Ethernet hub error messages.

**Error Message**

%HUB-1-BADHUB: Invalid hub type [dec] and number [dec]

**Explanation** An internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HUB-1-BADUNIT: Bad port number [dec]

**Explanation** An internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HUB-1-NOMEMORY: Unit [dec], no memory for [chars]

**Explanation** The system has detected that there is not enough memory for the hub initialization.

**Recommended Action** Reduce other system activity to ease memory demands. If conditions warrant, upgrade to a larger memory configuration.

**Error Message**

%HUB-1-READERR: Read op [dec] not allowed

**Explanation** An internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%HUB-1-WRITEERR: Write op [dec] not allowed

**Explanation** An internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## HW\_VPN Messages

The following are Encryption Advanced Interface Module (EAIM) error messages. EAIM is a hardware accelerator for IPsec encryption services.

**Error Message**

%HW\_VPN-1-BADMEMSIZE: [chars]: Invalid Amount of RAM for PA ID, memsize = [hex]

**Explanation** The POST has reported an incorrect memory size.

**Recommended Action** Replace the EAIM.

**Error Message**

%HW\_VPN-1-BADTYPE: This Encryption AIM type not supported on this router platform

**Explanation** An EAIM that is not supported on this router platform has been installed. Different EAIMs are supported by each router platform.

**Recommended Action** Remove the EAIM and install an EAIM that is compatible with this router.

**Error Message**

%HW\_VPN-1-BUSY: Encryption AIM busy

**Explanation** The EAIM cannot perform the requested command because it is busy executing another command.

**Recommended Action** Wait until the current command has completed. If the current command does not complete in a reasonable amount of time, the EAIM is defective. Replace the EAIM.

**Error Message**

%HW\_VPN-1-CMDERR: [chars]: Command [hex] failed with status [hex]

**Explanation** The EAIM has responded that the current requested command contains an error, and the command has failed. The details of the failure depend upon the circumstances, but it is likely that the EAIM is defective and should be replaced.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information. The EAIM will most likely need to be replaced.

**Error Message**

%HW\_VPN-1-CMDTIMEOUT: [chars]: Timeout on reply to command to Encryption AIM

**Explanation** The EAIM has not responded to the current requested command in a reasonable amount of time. The EAIM is faulty and should be replaced.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information. The EAIM will most likely need to be replaced.

**Error Message**

%HW\_VPN-1-DEVID: EAIM: Invalid PCI device ID: [int]

**Explanation** The identity of the EAIM device on the router bus is invalid.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information. The EAIM will need to be replaced.

**Error Message**

%HW\_VPN-1-DEVINIT: EAIM: Device Initialization failure

**Explanation** The EAIM has failed to respond properly to an initialization attempt.

**Recommended Action** Replace the EAIM.

**Error Message**

%HW\_VPN-6-DISABLED: [chars]: disabled

**Explanation** The EAIM has been disabled.

**Recommended Action** Replace the EAIM.

**Error Message**

%HW\_VPN-1-ELMERREV: AIM in slot [int] not supported by this HW revision.

**Explanation** The revision level of the C2600 PLD does not support EAIM. The PLD needs to be upgraded to a later version of software.

**Recommended Action** Upgrade the PLD software to a later version that supports EAIM.

**Error Message**

%HW\_VPN-1-HELLOERR: [chars]: EAIM responded incorrectly to hello: received [hex] expected [hex]

**Explanation** The EAIM should have echoed back the data that was sent to it via a command. Instead of receiving the expected data, the data that is specified in the error message text was received.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information. The EAIM will most likely need to be replaced.

**Error Message**

%HW\_VPN-1-HPRXERR: [chars]: Packet Encryption/Decryption error, status=[int]

**Explanation** An unexpected error occurred during the encryption or decryption of a packet.

**Recommended Action** This message may occur during the normal operation of the system, or it may occur during the transition to a new session key for a security association. In such cases, it may be ignored. However, if it happens frequently, or is associated with traffic disruption, make a note of the status value and contact your Cisco technical support representative. The EAIM will most likely need to be replaced.

**Error Message**

%HW\_VPN-1-INITFAIL: EAIM: Initialization failed at [chars]

**Explanation** The EAIM device did not reset properly. This condition is indicative of a hardware failure.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information. The EAIM will need to be replaced.

**Error Message**

%HW\_VPN-1-LPRXERR: [chars]: Key management error, cmd=[hex] status=[hex]

**Explanation** An unexpected error has occurred during the execution of a key management command by the EAIM.

**Recommended Action** Make a note of the status value and contact your Cisco technical support representative. The EAIM will most likely need to be replaced.

**Error Message**

%HW\_VPN-6-MULTDEV: Cannot support more than one Encryption AIMS

**Explanation** A second EAIM was discovered in the system. The Encryption AIM software supports only a single EAIM. All other EAIMs installed will be ignored.

**Recommended Action** Remove one of the EAIMs that is installed in your system.

**Error Message**

%HW\_VPN-1-NOHW: Encryption AIM not present in system

**Explanation** The user entered a command that involves an EAIM, but no EAIM is present in the system.

**Recommended Action** Do not enter EAIM commands unless an EAIM is present. If an EAIM is installed, replace the EAIM.

**Error Message**

%HW\_VPN-1-POSTFAIL: [chars]: Power On Self Test failed, alert status = [hex]

**Explanation** The POST for the EAIM has failed.

**Recommended Action** Replace the EAIM.

**Error Message**

%HW\_VPN-6-STARTUP: [chars]: starting up

**Explanation** The specified EAIM has initialized successfully.

**Recommended Action** This is an informational message only. No action is required.

**Error Message**

%HW\_VPN-1-UNEXPCMD: [chars]: Invalid command reply: expected [hex] received 0x[chars]

**Explanation** A command was sent to the EAIM, and its reply contained an unexpected reply code. The details of the failure depend upon the circumstances, but in all likelihood the Encryption AIM is faulty and should be replaced.

**Recommended Action** Make a note of the error message and contact your Cisco technical support representative. The EAIM will most likely need to be replaced.

# I82543 Messages

The following are Intel 82543 Ethernet/Fast Ethernet/Gigabit Ethernet controller error messages.

## Error Message

%I82543-1-DISCOVER: Only found [dec] interfaces on bay [dec], shutting down bay

**Explanation** A possible hardware error has occurred that resulted in too few GE interfaces being discovered.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** command output, contact your Cisco technical support representative and provide the representative with the gathered information.

## Error Message

%I82543-3-ERRINT: [chars], error interrupt, csr\_STATUS=[hex]

**Explanation** The Intel 82543 controller has signaled an error condition.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## Error Message

%I82543-1-INITFAIL\_NOMEM: [chars], initialization failed, no buffer memory

**Explanation** The Ethernet port initialization has failed because of insufficient memory.

**Recommended Action** Upgrade the affected PA with a larger memory model. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## Error Message

%I82543-5-LOSTCARR: [chars] cable/transceiver problem?

**Explanation** The Ethernet port has detected a link failure. The Ethernet port is no longer receiving signals from the LAN. This condition can be caused by disconnected Ethernet cabling, a transceiver (GBIC) failure, or a remote end that has been shut down.

**Recommended Action** Check your Ethernet wiring and port adapter. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%I82543-2-NOISL: Interface [chars] does not support ISL

**Explanation** ISL is not supported on the specified interface hardware.

**Recommended Action** No action is required.

**Error Message**

%I82543-3-NOTI82543: PA bay [int], device number [int]: unknown device ([hex])

**Explanation** The PA does not contain an Intel 82543 controller chip.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** command output, contact your Cisco technical support representative and provide the representative with the gathered information.

**Error Message**

%I82543-3-TOOBIG: [chars], packet too big ([dec]), from [enet]

**Explanation** The interface has detected a packet that is a larger size than the size that has been defined by the MTU.

**Recommended Action** Check the MTU setting of the other station. No action is required.

## IBM2692 Messages

The following are IBM Token Ring chipset error messages.

**Error Message**

%IBM2692-1-DISCOVER: Only found [dec] interfaces on bay [dec], shutting down bay

**Explanation** One of the interface controller devices on the module did not initialize properly.

**Recommended Action** Power down, reinsert the network module, and reboot the system. If this message recurs, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%IBM2692-1-LL\_QUEUE\_OVERFLOW: IBM2692 ([dec]/[dec]), LL queue overflow.

**Explanation** A packet buffer queue has overflowed and a packet was lost, probably because of traffic congestion.

**Recommended Action** A small number of queue overflows might not be a cause for concern. Reducing the load on the router or installing a higher performance router should alleviate queue overflows.

**Error Message**

```
%IBM2692-1-NOPCIMEMORY: [chars] [chars] creation failed
```

**Explanation** The router or access server could not allocate memory for the specified descriptors.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

```
%IBM2692-1-OLDREV: Bay [dec] port adapter requires Rev 2 CPU
```

**Explanation** The Token Ring PCI Port Adapter driver depends on the capabilities of the Revision 2 processor.

**Recommended Action** Upgrade the processor to Revision 2.

**Error Message**

```
%IBM2692-1-SRBQ_OVERFLOW: Queue size on [chars] exceeded [dec]
```

**Explanation** The maximum number of commands that can be queued to the Token Ring port has been exceeded. Normally, such a problem is temporary, depending on transient peak loads within the system.

**Recommended Action** The system should recover. No action is required.

## ICC Messages

The following are Inter-Card Communication (ICC) error messages.

**Error Message**

```
%ICC-4-COMM: Communication failure occurred while [chars]
```

**Explanation** A communication failure has occurred between the specified card and another card in the system.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** command output, contact your Cisco technical support representative and provide the representative with the gathered information.

**Error Message**

%ICC-4-CONSISTENCY: Internal consistency check: [chars]

**Explanation** An internal inconsistency was found in some ICC data structures.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** command output, contact your Cisco technical support representative and provide the representative with the gathered information.

**Error Message**

%ICC-4-HEARTBEAT: Card [dec] failed to respond to heartbeat

**Explanation** A communication failure between the primary and the specified line card has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** command output, contact your Cisco technical support representative and provide the representative with the gathered information.

**Error Message**

%ICC-2-NOMEM: No memory available for [chars]

**Explanation** The ICC subsystem could not obtain sufficient memory.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** command output, contact your Cisco technical support representative and provide the representative with the gathered information.

## IDBINDEX\_SYNC Messages

The following are Interface Descriptor Block (IDB) index synchronization messages.

**Error Message**

%IDBINDEX\_SYNC-3-IDBINDEX\_ENTRY\_DEL: Cannot delete entry from interface index table: "[chars]", [dec]

**Explanation** An interface index table entry is not deleted from the interface index table due to an internal software error.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. With some messages, these tools and utilities will supply clarifying information. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case

with the Technical Assistance Center via the Internet <http://tools.cisco.com/ServiceRequestTool/create>, or contact your Cisco technical support representative and provide the representative with the gathered information. Provide the output of the `show running-config`, `show logging`, `show monitor event-trace ifnum merged all`, `show ifnum list`, `show ifnum statistics`, `show cef idb` and `show cef interface` commands. Also provide the sequence of commands that was used to reproduce the error.

#### Error Message

```
%IDBINDEX_SYNC-3-IDBINDEX_ENTRY_MISMATCH: An interface index mismatched its active table entry: "[chars]"
```

**Explanation** An interface index was found which did not match the active interface index table entry with the corresponding synchronization key due to an internal software error.

**Recommended Action** LOG\_STD\_ACTION.

#### Error Message

```
%IDBINDEX_SYNC-3-IDBINDEX_ENTRY_SET: Cannot set entry to interface index table: "[chars]", [dec]
```

**Explanation** An interface index table entry is not set to the interface index table due to an internal software error.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. With some messages, these tools and utilities will supply clarifying information. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet <http://tools.cisco.com/ServiceRequestTool/create>, or contact your Cisco technical support representative and provide the representative with the gathered information. Provide the output of the `show running-config`, `show logging`, `show monitor event-trace ifnum merged all`, `show ifnum list`, `show ifnum statistics`, `show cef idb` and `show cef interface` commands. Also provide the sequence of commands that was used to reproduce the error.

#### Error Message

```
%IDBINDEX_SYNC-3-INIT_ERR: [chars]
```

**Explanation** The interface index synchronization ISSU client has an initialization error.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. With some messages, these tools and utilities will supply clarifying information. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet <http://tools.cisco.com/ServiceRequestTool/create>, or contact your Cisco technical support representative and provide the representative with the gathered information. Provide the output of the `show running-config`, `show logging`, `show monitor event-trace ifnum merged all`, `show ifnum list`, `show ifnum statistics`, `show cef idb` and `show cef interface` commands. Also provide the sequence of commands that was used to reproduce the error.

**Error Message**

%IDBINDEX\_SYNC-3-IPC\_ERR: [chars]: [chars].

**Explanation** The interface index synchronization IPC session has an error.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. With some messages, these tools and utilities will supply clarifying information. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet <http://tools.cisco.com/ServiceRequestTool/create>, or contact your Cisco technical support representative and provide the representative with the gathered information. Provide the output of the **show running-config**, **show logging**, **show monitor event-trace ifnum merged all**, **show ifnum list**, **show ifnum statistics**, **show cef idb** and **show cef interface** commands. Also provide the sequence of commands that was used to reproduce the error.

**Error Message**

%IDBINDEX\_SYNC-3-ISSU\_ERR: [chars][chars], rc=[dec]

**Explanation** The interface index synchronization ISSU client has an error.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. With some messages, these tools and utilities will supply clarifying information. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet <http://tools.cisco.com/ServiceRequestTool/create>, or contact your Cisco technical support representative and provide the representative with the gathered information. Provide the output of the **show running-config**, **show logging**, **show monitor event-trace ifnum merged all**, **show ifnum list**, **show ifnum statistics**, **show cef idb** and **show cef interface** commands. Also provide the sequence of commands that was used to reproduce the error.

**Error Message**

%IDBINDEX\_SYNC-3-RF\_ERR: [chars] [dec].

**Explanation** The interface index synchronization RF client has error.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. With some messages, these tools and utilities will supply clarifying information. Also perform a search of the Bug Toolkit <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. If you still require assistance, open a case with the Technical Assistance Center via the Internet <http://tools.cisco.com/ServiceRequestTool/create>, or contact your Cisco technical support representative and provide the representative with the gathered information. Provide the output of the **show running-config**, **show logging**, **show monitor event-trace ifnum merged all**, **show ifnum list**, **show ifnum statistics**, **show cef idb** and **show cef interface** commands. Also provide the sequence of commands that was used to reproduce the error.

# IDMGR Messages

The following are ID manager error messages.

## Error Message

%IDMGR-3-INTERRUPT: [chars]

**Explanation** A id\_get operation has been attempted at the interrupt level.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## Error Message

%IDMGR-3-INVALID\_ID: bad id in [chars]

**Explanation** An ID manager error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## Error Message

%IDMGR-3-MALLOC\_FAILURE: [chars]

**Explanation** A memory allocation failure has occurred in the ID manager.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

# IDS Messages

The following are IP datagram subsystem (IDS) error messages.

## Error Message

%IDS-4-ICMP\_ECHO\_REPLY\_SIG: Sig:2000:ICMP Echo Reply - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0 (Echo Reply). This condition is extremely common as a part of network traffic; however, suspicion should be aroused when a large number of these packets are found on the network.

**Recommended Action** If no legitimate reason for this traffic can be identified, perform prudent security measures and, if necessary, block the host that sent this datagram.

**Error Message**

%IDS-4-ICMP\_ECHO\_SIG: Sig:2004:ICMP Echo Request - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request). This type of datagram is commonly used to perform reconnaissance sweeps. The ICMP Echo Request is issued by the source to determine if the destination is “alive.” When the destination receives the request, it will reply with an ICMP Echo Reply. This request and reply pair is most commonly implemented via the ping utility. Many network management tools use this utility or some derivative of it, and this condition is extremely common as a part of network traffic. However, suspicion should be aroused when a large number of these packets are found on the network.

**Recommended Action** If no legitimate reason for this traffic can be identified, perform prudent security measures and, if necessary, block the host that sent this datagram.

**Error Message**

%IDS-4-ICMP\_FRAGMENT\_SIG: Sig:2150:Fragmented ICMP Traffic - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag set to 1 (ICMP) or an offset has been indicated in the offset field. IP datagrams may be fragmented normally as they are transported across the network, but ICMP is rarely fragmented. The traffic should be investigated.

**Recommended Action** If no legitimate reason for the fragmentation can be found and, especially, if the packets seem to be originating from a single source, perform prudent security measures and, if necessary, block the host that sent this datagram.

**Error Message**

%IDS-4-ICMP\_INFO\_REPLY\_SIG: Sig:2010:ICMP Information Reply - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply). No known exploit exists. This datagram type is obsolete and should not be encountered.

**Recommended Action** When nonspecific network traffic of this type is encountered, the best action from a security perspective is to block or disallow the host that sent this datagram. If the source of this datagram is legitimate, the source of the datagram will identify itself.

**Error Message**

%IDS-4-ICMP\_INFO\_SIG: Sig:2009:ICMP Information Request - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request). This datagram type is obsolete and should not be encountered.

**Recommended Action** When nonspecific network traffic of this type is encountered, the best action from a security perspective is to block or disallow the host that sent this datagram. If the source of this datagram is legitimate, the source of the datagram will identify itself.

**Error Message**

%IDS-4-ICMP\_MASK\_REPLY\_SIG: Sig:2012:ICMP Address Mask Reply - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply). No known exploits incorporate this option. The ICMP Address Mask Request and Reply pair can be used to determine the subnet mask used on the network. When the requesting system issues the Address Mask Request bound for a destination, the destination system responds with an Address Mask Reply message. This condition can sometimes be a part of normal network traffic, but is uncommon on most networks. Suspicion should be aroused when a large number of these packets are found on the network.

**Recommended Action** If no legitimate reason for the traffic can be found and, especially, if the packets seem to be originating from a single source, perform prudent security measures and, if necessary, block the host that sent this datagram.

**Error Message**

%IDS-4-ICMP\_MASK\_SIG: Sig:2011:ICMP Address Mask Request - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request). ICMP Address Mask Requests could be used to perform reconnaissance sweeps of networks. The ICMP Address Mask Request and Reply pair can be used to determine the subnet mask used on the network. When the requesting system issues the Address Mask Request bound for a destination, the destination system responds with an Address Mask Reply message. This condition can sometimes be a part of normal network traffic, but is uncommon on most networks. Suspicion should be aroused when a large number of these packets are found on the network.

**Recommended Action** If no legitimate reason for the traffic can be found, perform prudent security measures and, if necessary, block the host that sent this datagram.

**Error Message**

%IDS-4-ICMP\_PARAMPROB\_SIG: Sig:2006:ICMP Parameter Problem on Datagram - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram). No known exploits incorporate this option. ICMP Parameter Problem datagrams are issued when a router has had to drop

a malformed datagram. This condition is a normal and necessary type of network traffic; however, large numbers of this datagram type on the network can be indicative of network difficulties or hostile actions.

**Recommended Action** If no network problems can be identified to account for the traffic, perform prudent security measures and, if necessary, block the host that sent this datagram.

#### Error Message

```
%IDS-4-ICMP_PING_OF_DEATH_SIG: Sig:2154:ICMP Ping of Death Attack - from  
[IP_address] to [IP_address]
```

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP), the Last Fragment bit is set, and  $(\text{IP offset} * 8) + (\text{IP data length})$  is greater than 65535. In other words, the IP offset (which represents the starting position of this fragment in the original packet, and which is byte units) plus the rest of the packet is greater than the maximum size for an IP packet. This condition indicates a denial-of-service attack.

**Recommended Action** It is likely that the source address has been spoofed, making it ineffective to block the host that sent this datagram. Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

#### Error Message

```
%IDS-4-ICMP_REDIRECT_SIG: Sig:2003:ICMP Redirect - from [IP_address] to  
[IP_address]
```

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect). The redirect message may be issued from a router to inform a host of a better route to a requested destination. The host then updates its routing table to include this route. This method of updating routing tables is an uncommon practice today.

**Recommended Action** When nonspecific network traffic of this type is encountered, the best action from a security perspective is to block or disallow the host that sent this datagram. If the source of this datagram is legitimate, the source of the datagram will identify itself.

#### Error Message

```
%IDS-4-ICMP_SOURCEQUENCH_SIG: Sig:2002:ICMP Source Quench - from [IP_address] to  
[IP_address]
```

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench). This datagram may be used in network management to provide congestion control. Large numbers of this datagram type on the network are indicative of network difficulties or may be indicative of hostile actions. This datagram may be used in network management to provide congestion control. A source quench packet will be issued when a router is beginning to lose packets due to the transmission rate of a source. The source quench is a request to the source to reduce the rate of datagram transmission. This datagram type is

rarely, if ever, seen on networks and some systems do not even support it. Large numbers of this datagram type on the network are indicative of network difficulties or may be indicative of hostile actions.

**Recommended Action** If no network problems can be identified to account for the traffic, perform prudent security measures to block the host that sent this datagram.

#### Error Message

%IDS-4-ICMP\_TIME\_REPLY\_SIG: Sig:2008:ICMP Timestamp Reply - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply). No known exploits incorporate this option. The ICMP Timestamp Request and Reply pair can be used to synchronize system clocks on the network. The requesting system issues the Timestamp Request bound for a destination, and the destination system responds with a Timestamp Reply message. This condition can sometimes be a part of normal network traffic, but is uncommon on most networks. Suspicion should be aroused when a large number of these packets are found on the network.

**Recommended Action** If no legitimate reason for this traffic can be identified, perform prudent security measures to block the host that sent this datagram.

#### Error Message

%IDS-4-ICMP\_TIME\_SIG: Sig:2007:ICMP Timestamp Request - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request). ICMP Timestamp Requests could be used to perform reconnaissance sweeps of networks. No known exploits incorporate this option. The ICMP Timestamp Request and Reply pair can be used to synchronize system clocks on the network. The requesting system issues the Timestamp Request bound for a destination, and the destination system responds with a Timestamp Reply message. This condition is normal as a part of network traffic, but is uncommon on most networks. Suspicion should be aroused when a large number of these packets are found on the network.

**Recommended Action** If no legitimate reason for this traffic can be identified, perform prudent security measures to block the host that sent this datagram.

#### Error Message

%IDS-4-ICMP\_TIMXCEED\_SIG: Sig:2005:ICMP Time Exceeded for a Datagram - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11 (Time Exceeded for a Datagram). No known exploits incorporate this option. ICMP Time Exceeded datagrams are issued when a router has had to drop a datagram whose TTL flag has expired. This condition is a normal and necessary type of network traffic. However, large numbers of this datagram type on the network are indicative of network difficulties or may be indicative of hostile actions.

**Recommended Action** If no network problems can be identified to account for the traffic, perform prudent security measures to block the host that sent this datagram.

**Error Message**

%IDS-4-ICMP\_TOOLARGE\_SIG: Sig:2151:Large ICMP Traffic - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with a size greater than 1024 bytes. Although it is possible to receive ICMP datagrams that have a size greater than 1024 bytes, this condition is a highly unusual occurrence that warrants investigation.

**Recommended Action** If no legitimate reason for the large packet size can be found and, especially, if the packets seem to be originating from a single source, perform prudent security measures to block the host that sent this datagram.

**Error Message**

%IDS-4-ICMP\_UNREACH\_SIG: 2001:ICMP Host Unreachable - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable). This type of datagram is the common response provided to a client when there is no path available to the requested host and is a very common type of network traffic. However, large numbers of this datagram type on the network are indicative of network difficulties or may be indicative of hostile actions.

**Recommended Action** If no network problems can be identified to account for the traffic, perform prudent security measures to block the host that sent this datagram.

**Error Message**

%IDS-4-IPFRAG\_ATTACK\_SIG: Sig:1100:IP Fragment Attack - from [IP\_address] to [IP\_address]

**Explanation** Any IP datagram has been received with the “more fragments” flag set to 1 or if there is an offset indicated in the offset field.

**Recommended Action** IP datagrams may be fragmented normally when they are transported across the network. This condition is common, but is unusual enough that the traffic should be investigated, especially if the network is protected by a packet-filtering firewall.

**Error Message**

%IDS-4-IP\_IMPOSSIBLE\_SIG: Sig:1102:Impossible IP Packet - from [IP\_address] to [IP\_address]

**Explanation** An IP packet has arrived with a source address that is the same as the destination address. This message will detect the so-called Land Attack.

**Recommended Action** This condition should never occur in legitimate traffic.

**Error Message**

%IDS-4-IPOPT\_LSRR\_SIG: Sig:1004:IP options-Loose Source Route - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received in which the IP option list for the datagram includes option 3 (Loose Source Route). This option may be misused to defeat authentication mechanisms that rely on IP addresses as their basis for trust relationships. Although network troubleshooting may require the legitimate use of this feature, this type of traffic is rarely, if ever, noted and should make up much less than 1 percent of network traffic.

**Recommended Action** Small amounts of source routed traffic probably indicate that a network problem is being investigated. Large amounts of source routed traffic is more suspicious and a thorough investigation of the source and reason should be performed.

**Error Message**

%IDS-4-IPOPT\_RR\_SIG: Sig:1001:IP options-Record Packet Route - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with an IP option list that contains one or more options that perform various network management or debugging tasks. This alarm may indicate that a reconnaissance attack is in progress against your network. Although network troubleshooting may require the legitimate use of this feature, this is unusual traffic that should be investigated.

**Recommended Action** When nonspecific network traffic of this type is encountered, perform prudent security measures to block or disallow the source of the datagram. If the source of this datagram is legitimate, the source of the datagram will identify itself.

**Error Message**

%IDS-4-IPOPT\_SATID\_SIG: Sig:1005:IP options-SATNET ID - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received in which the IP option list for the datagram includes option 8 (SATNET stream identifier). No known exploit exists. This option is obsolete and should not be encountered.

**Recommended Action** When nonspecific network traffic of this type is encountered, perform prudent security measures to block or disallow the source of the datagram. If the source of this datagram is legitimate, the source of the datagram will identify itself.

**Error Message**

%IDS-4-IPOPTS\_BAD\_SIG: Sig:1000:Bad IP Option List - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received in which the list of IP options in the IP datagram header is incomplete or malformed. No known exploits purposely incorporate this option. There is no legitimate use for malformed datagrams. This malformed datagram may indicate systems that are experiencing problems with their kernel or NIC. This condition is indicative of unusual traffic and warrants investigation.

**Recommended Action** When nonspecific network traffic of this type is encountered, perform prudent security measures to block or disallow the source of the datagram. If the source of this datagram is legitimate, the source of the datagram will identify itself.

**Error Message**

%IDS-4-IPOPT\_SECURITY\_SIG: Sig:1003:IP options-Provide s,c,h,tcc - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received in which the IP option list for the datagram includes option 2. No known exploit exists. This message appears if IP security options have been implemented on your network. However, these options are rarely, if ever, implemented.

**Recommended Action** When nonspecific network traffic of this type is encountered, perform prudent security measures to block or disallow the source of the datagram. If the source of this datagram is legitimate, the source of the datagram will identify itself.

**Error Message**

%IDS-4-IPOPT\_SSRR\_SIG: Sig:1006:IP options-Strict Source Route - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received in which the IP option list for the datagram includes option 2 (Strict Source Routing). This option may be misused to defeat authentication mechanisms that rely on IP addresses as their basis for trust relationships. Although network troubleshooting may require the legitimate use of this feature, this type of traffic is rarely, if ever, noted and should make up much less than 1 percent of network traffic.

**Recommended Action** Small amounts of source routed traffic probably indicates a network problem that is being investigated. Large amounts of source routed traffic is more suspicious, and the source of, and reason for, this datagram should be investigated.

**Error Message**

%IDS-4-IPOPT\_TS\_SIG: Sig:1002:IP options-TimeStamp - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received in which the IP option list for the datagram includes option 4 (Timestamp). This alarm indicates that a reconnaissance attack may be in progress against your network. Although network troubleshooting may require the legitimate use of this feature, this is unusual traffic and should be investigated.

**Recommended Action** When nonspecific network traffic of this type is encountered, perform prudent security measures to block or disallow the source of the datagram. If the source of this datagram is legitimate, the source of the datagram will identify itself.

**Error Message**

%IDS-4-IP\_UNKNOWN\_PROTO\_SIG: Sig:1101:Unknown IP Protocol - from [IP\_address] to [IP\_address]

**Explanation** An IP datagram has been received with the protocol field set to 101 or greater. The use of these protocol types is highly unusual and should be investigated.

**Recommended Action** When nonspecific network traffic of this type is encountered, perform prudent security measures to block or disallow the source of the datagram. If the source of this datagram is legitimate, the source of the datagram will identify itself.

**Error Message**

%IDS-4-LOST\_CONNECT: Connection to HostID:[int] OrgID:[int]

**Explanation** A connection has been dropped, but there was no previous connection. Locally developed protocols that use these protocol types will trigger this message. The use of these protocol types is highly unusual and should be investigated.

**Recommended Action** IDS cannot communicate with the Director. Check the connectivity to the Director and check the post office configuration on both the router and the Director.

**Error Message**

%IDS-4-RPC\_CALLIT\_REQUEST: Sig:6103:Proxied RPC Request - from [IP\_address] to [IP\_address]

**Explanation** A proxied RPC request has been sent to the portmapper of a target host.

**Recommended Action** If this procedure is allowed on your network, users who employ it will trigger this message. This condition may be a serious attempt at gaining unauthorized access. If the source of the attempt is not within your network, it should be blocked.

**Error Message**

%IDS-4-RPC\_DUMP\_REQUEST: Sig:6102:RPC Dump - from [IP\_address] to [IP\_address]

**Explanation** An RPC dump request has been issued to a target host. This is a common procedure performed by many system administrators and wary users to determine which RPC services are being offered. Executing this procedure is most likely due to curiosity on the part of a novice user or due to a system administrator performing system maintenance.

**Recommended Action** If upon investigation no valid user can be associated with this event, perform prudent security measures to block the source of this RPC dump request.

**Error Message**

%IDS-4-RPC\_PORTREQ\_MOUNTD: Sig:6155:RPC mountd Portmap Request - from [IP\_address] to [IP\_address]

**Explanation** A request has been made to the portmapper for the mount daemon (mountd) port. If this procedure is allowed on your network, users who employ it will trigger this message.

**Recommended Action** This request may be a serious attempt to gain unauthorized access. If the source of the attempt is not within your network, block the source of this request.

**Error Message**

%IDS-4-RPC\_PORTREQ\_REXD: Sig:6175:RPC rexd Portmap Request - from [IP\_address] to [IP\_address]

**Explanation** A request has been made to the portmapper for the remote execution daemon (rex) port. The remote execution daemon is the server responsible for remote program execution. This condition may indicate an attempt to gain unauthorized access to system resources. If this procedure is allowed on your network, users who employ it will trigger this message.

**Recommended Action** This request may be a serious attempt to gain unauthorized access. If the source of the attempt is not within your network, block the source of this request.

**Error Message**

%IDS-4-RPC\_PORTREQ\_YPBIND: Sig:6151:RPC ypbind Portmap Request - from [IP\_address] to [IP\_address]

**Explanation** A request has been made to the portmapper for the YP bind daemon (ypbind) port. If this procedure is allowed on your network, users who employ it will trigger this message.

**Recommended Action** This request may be a serious attempt to gain unauthorized access. If the source of the attempt is not within your network, block the source of this request.

**Error Message**

%IDS-4-RPC\_PORTREQ\_YPPASSWDD: Sig:6152:RPC ypbind yppasswdd Portmap Request - from [IP\_address] to [IP\_address]

**Explanation** A request has been made to the portmapper for the YP password daemon (yppasswdd) port. If this procedure is allowed on your network, users who employ it will trigger this message.

**Recommended Action** This request may be a serious attempt to gain unauthorized access. If the source of the attempt is not within your network, block the source of this request.

**Error Message**

%IDS-4-RPC\_PORTREQ\_YPSERV: Sig:6150:RPC ypserv Portmap Request - from [IP\_address] to [IP\_address]

**Explanation** A request has been made to the portmapper for the YP server daemon (ypserv) port. If this procedure is allowed on your network, users who employ it will trigger this message.

**Recommended Action** This request may be a serious attempt to gain unauthorized access. If the source of the attempt is not within your network, block the source of this request.

**Error Message**

%IDS-4-RPC\_PORTREQ\_YPUPDATED: Sig:6153:RPC ypupdated Portmap Request - from [IP\_address] to [IP\_address]

**Explanation** A request has been made to the portmapper for the YP update daemon (ypupdated) port. If this procedure is allowed on your network, users who employ it will trigger this message.

**Recommended Action** This request may be a serious attempt to gain unauthorized access. If the source of the attempt is not within your network, block the source of this request.

**Error Message**

%IDS-4-RPC\_PORTREQ\_YPXFRD: Sig:6154:RPC ypxfrd Portmap Request - from [IP\_address] to [IP\_address]

**Explanation** A request has been made to the portmapper for the YP transfer daemon (ypxfrd) port. If this procedure is allowed on your network, users who employ it will trigger this message.

**Recommended Action** This request may be a serious attempt to gain unauthorized access. If the source of the attempt is not within your network, block the source of this request.

**Error Message**

%IDS-4-RPC\_REXD\_REQUEST: Sig:6180:RPC rexd Attempt - from [IP\_address] to [IP\_address]

**Explanation** A call to the rexd program has been made. The remote execution daemon is the server responsible for remote program execution. This procedure may be indicative of an attempt to gain unauthorized access to system resources. Even if this service is being used legitimately, this alarm will occur.

**Recommended Action** For security purposes, this service should not be used.

**Error Message**

%IDS-4-RPC\_SET\_REQUEST: Sig:6100:RPC Port Registration - from [IP\_address] to [IP\_address]

**Explanation** Attempts have been made to register new RPC services on a target host. No benign triggers exist for this message.

**Recommended Action** Perform prudent security practices and block the source of this attempt.

**Error Message**

%IDS-4-RPC\_STATD\_OVFLW: Sig:6190:statd Buffer Overflow - from [IP\_address] to [IP\_address]

**Explanation** A large statd request has been sent.

**Recommended Action** This message should not be seen in legitimate traffic.

**Error Message**

%IDS-4-RPC\_UNSET\_REQUEST: Sig:6101:RPC Port Unregistration - from [IP\_address] to [IP\_address]

**Explanation** Attempts have been made to unregister new RPC services on a target host. No benign triggers exist for this message.

**Recommended Action** Perform prudent security practices and block the source of this attempt.

**Error Message**

%IDS-4-STR\_MATCH\_SIG: Sig:8000:FTP Retrieve Password File - from [IP\_address] to [IP\_address]

**Explanation** The string “passwd” has been issued during an FTP session. Although system administrators might use this service to update system files, issuing the string “passwd” on a regular basis is a high security risk and should be avoided. No other benign triggers exist for this message.

**Recommended Action** If, after investigation, the alarm was not generated by a system administrator, perform prudent security practices and block the source of the string.

**Error Message**

%IDS-4-TCP\_FIN\_ONLY\_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from [IP\_address] to [IP\_address]

**Explanation** A TCP packet has been received with the FIN bit set but with no ACK bit set in the flags field. There is no legitimate use for malformed TCP datagrams. This condition is indicative of unusual network traffic and warrants investigation. Hacker tools will generate TCP packets with the FIN bit set but with no ACK bit set in the flags field in an attempt to elude intrusion detection.

**Recommended Action** When nonspecific network traffic of this type is encountered, the best action from a security perspective is to block or disallow the host that sent this TCP packet. If the source of this packet is legitimate, the source of the packet will identify itself.

**Error Message**

%IDS-4-TCP\_FTP\_CWDROOT\_SIG: Sig:3152:FTP CWD ~root - from [IP\_address] to [IP\_address]

**Explanation** A user has attempted to execute the **cwd ~root** command. There is no known reason why this command should ever be executed.

**Recommended Action** If this message is triggered from a source outside of your network perform prudent security practices and block the source of the request.

**Error Message**

%IDS-4-TCP\_FTP\_PORT\_BADADDR\_SIG: Sig:3153:FTP Improper Address Specified - from [IP\_address] to [IP\_address]

**Explanation** A port command has been issued with an address that is not the same as the requesting host.

**Recommended Action** No action is required.

**Error Message**

%IDS-4-TCP\_FTP\_PORT\_BADPORT\_SIG: Sig:3154:FTP Improper Port Specified - from [IP\_address] to [IP\_address]

**Explanation** A port command has been issued with a data port specified that is less than 1024 bytes or greater than 65535 bytes.

**Recommended Action** No action is required.

**Error Message**

%IDS-4-TCP\_FTP\_SITE\_SIG: Sig:3150:FTP Remote Command Execution - from [IP\_address] to [IP\_address]

**Explanation** A user has attempted to execute the FTP **site** command. The **site** command allows a user to execute a limited number of commands via the FTP server on the host machine. No authentication is required to execute the **site** command. The commands that may be executed vary from system to system and on many systems the **site** command is not implemented.

**Recommended Action** Disable the **site** command on the FTP servers, if possible. If this message is triggered by a source outside of your network, perform prudent security measures and block the source of this FTP **site** command.

**Error Message**

%IDS-4-TCP\_FTP\_SYST\_SIG: Sig:3151:FTP SYST Command Attempt - from [IP\_address] to [IP\_address]

**Explanation** A user has attempted to execute the FTP **syst** command. The **syst** command returns the type of operating system that the FTP server is running. Authentication is not required to execute this command. The **syst** command provides information that may be used to refine attack methods. An FTP from a Linux session will cause the **syst** message to appear. Some proxies, such as the TIS Toolkit, issue the **syst** command as a matter of course.

**Recommended Action** Use an FTP version that has the **syst** command disabled.

**Error Message**

%IDS-4-TCP\_MAJORDOMO\_EXEC\_BUG: Sig:3107:Majordomo Execute Attack - from [IP\_address] to [IP\_address]

**Explanation** Because of a bug in the Majordomo program, a remote user has attempted to execute arbitrary commands at the privilege level of the server.

**Recommended Action** Perform prudent security measures and block the source of this attempt.

**Error Message**

%IDS-4-TCP\_NO\_FLAGS\_SIG: Sig:3040:TCP - No bits set in flags - from [IP\_address] to [IP\_address]

**Explanation** A TCP packet has been received with no bits set in the flags field. Hacker tools will generate TCP packets with no bits set in the flags field in an attempt to elude intrusion detection. There is no legitimate use for malformed TCP datagrams. This is unusual traffic and warrants an investigation.

**Recommended Action** When nonspecific network traffic of this type is encountered, the best action from a security perspective is to block or disallow the host that sent this TCP packet. If the source of this packet is legitimate, the source of the packet will identify itself.

**Error Message**

%IDS-4-TCP\_SENDMAIL\_BAD\_FROM\_SIG: Sig:3102:Sendmail Invalid Sender - from [IP\_address] to [IP\_address]

**Explanation** An e-mail message with a pipe (|) symbol in the From: field has been received. The presence of a pipe (|) in the From: field is a very serious indication that your network may be under attack.

**Recommended Action** Immediately block the source of the e-mail message. For security reasons, users should not be allowed to execute programs via e-mail servers.

**Error Message**

%IDS-4-TCP\_SENDMAIL\_BAD\_TO\_SIG: Sig:3101:Sendmail Invalid Recipient - from [IP\_address] to [IP\_address]

**Explanation** An e-mail message with a pipe (|) symbol in the recipient field has been received. The presence of a pipe (|) in the recipient field is a very serious indication that your network may be under attack.

**Recommended Action** Immediately block the source of the e-mail message. For security reasons, users should not be allowed to execute programs via e-mail servers.

**Error Message**

%IDS-4-TCP\_SENDMAIL\_BOUNCE\_SIG: Sig:3100:Smail Attack - from [IP\_address] to [IP\_address]

**Explanation** A very common “smail” attack against e-mail servers has occurred. This attack attempts to cause e-mail servers to execute programs on behalf of the attacker. This is a very serious indication that your network may be under attack.

**Recommended Action** Immediately block the source of the e-mail message. For security reasons, users should not be allowed to execute programs via e-mail servers.

**Error Message**

%IDS-4-TCP\_SENDMAIL\_DECODE: Sig:3105:Sendmail Decode Alias - from [IP\_address] to [IP\_address]

**Explanation** An e-mail message with “: decode@” in the header has been received. The decode alias is used to uudecode files and is primarily implemented as a convenience for system administration. If the decode alias is allowed to uudecode files, users who send e-mail to the alias will cause this message to appear.

**Recommended Action** For security purposes, the decode alias should not be allowed to uudecode files, and the service should be disabled. It is recommended that you block any hosts that attempt to send e-mail to this alias, especially if they are outside of your network.

**Error Message**

%IDS-4-TCP\_SENDMAIL\_INVALID\_COMMAND: Invalid SMTP command - from [IP\_address] to [IP\_address]

**Explanation** An invalid SMTP command in the SMTP connection has been entered. A suspicious violation that may be an attack to the mail server system has been detected.

**Recommended Action** Investigate the cause of the traffic.

**Error Message**

%IDS-4-TCP\_SENDMAIL\_OLD\_SIG: Sig:3104:Archaic Sendmail Attacks - from [IP\_address] to [IP\_address]

**Explanation** The **wiz** or **debug** command has been sent to the SMTP port. There is no reason for this type of traffic to be seen on modern networks.

**Recommended Action** Although there is little chance that there will be any adverse effects from someone attempting these old hacker commands, perform prudent security practices and block the source of this attempt.

**Error Message**

%IDS-4-TCP\_SENDMAIL\_SPAM\_SIG: Sig:3106:Excessive Rcpt to: (SPAM) - from [IP\_address] to [IP\_address]

**Explanation** An excessive number of "RCPT TO:" fields in the header of e-mail messages have been received. Some types of mailing list software may trigger this message.

**Recommended Action** No action is required.

**Error Message**

%IDS-4-TCP\_SENDMAIL\_VRFY\_SIG: Sig:3103:Sendmail Reconnaissance - from [IP\_address] to [IP\_address]

**Explanation** The **expn** or **vrfy** command has been issued to the SMTP port. These commands are commonly used to verify that a user e-mail account exists on the server or to expand an alias to determine who the actual recipients of a message may be. Users that use the **expn** and **vrfy** functions for legitimate purposes will trigger this message. The information that can be obtained from the **expn** and **vrfy** commands is useful, but not dangerous on its own.

**Recommended Action** Monitor future traffic for patterns of misuse.

**Error Message**

%IDS-4-TCP\_SYN\_ATTACK\_SIG: Sig:3050:Half-Open Syn Flood - from [IP\_address] to [IP\_address]

**Explanation** The number of half-open TCP connections has exceeded the high-water mark or the one minute high-rate mark. There are no known sources that would legitimately generate this traffic pattern. This condition may indicate some type of network problem and should be investigated.

**Recommended Action** To avoid depletion of your network resources, it is recommended that you block the source during the course of the investigation. If no network problems are discovered, perform prudent security practices and permanently block the host.

**Error Message**

%IDS-4-TCP\_SYN\_FIN\_SIG: Sig:3041:TCP - SYN and FIN bits set - from [IP\_address] to [IP\_address]

**Explanation** A TCP packet has been received with both the SYN and FIN bits set in the flags field. Hacker tools will generate TCP packets with the SYN and FIN bits set in the flags field in an attempt to elude intrusion detection. There is no legitimate use for malformed TCP datagrams. This condition is indicative of unusual traffic and warrants an investigation.

**Recommended Action** When nonspecific network traffic of this type is encountered, the best action from a security perspective is to block or disallow the host that sent this TCP packet. If the source of this packet is legitimate, the source of the packet will identify itself.

**Error Message**

%IDS-4-UDP\_BOMB\_SIG: Sig:4050:UDP Bomb - from [IP\_address] to [IP\_address]

**Explanation** The specified UDP length is less than the specified IP length. This malformed packet type is associated with a denial-of-service attempt. There is no legitimate use for malformed datagrams. This message may be indicative of systems that are experiencing problems with their kernel or NIC. This condition is indicative of unusual traffic and warrants an investigation.

**Recommended Action** When nonspecific network traffic of this type is encountered, the best action from a security perspective is to block or disallow the host that sent this packet. If the source of this packet is legitimate, the source of the packet will identify itself.

**Error Message**

%IDS-4-UDP\_TFTP\_PASSWD\_SIG: Sig:4100:Tftp Passwd File - from [IP\_address] to [IP\_address]

**Explanation** A user has attempted to use TFTP to obtain a password file. System administrators might use this service to update system files. Using TFTP to update system files on a regular basis is a high security risk and should be avoided. No other benign triggers exist for this message.

**Recommended Action** If, after investigation, the alarm was not generated by a system administrator, perform prudent security practices and block the source of this attempt.

## IDTATM25 Messages

The following are Integrated Digital Terminal (IDT) ATM25 network module error messages.

**Error Message**

%IDTATM25-1-DISCOVER: Only found [dec] interfaces on bay [dec], shutting down bay

**Explanation** The ATM25 network module hardware may be defective.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%IDTATM25-3-FAILSETUPVC: Interface [chars], Failed to setup vc [dec] (Cause: [chars])

**Explanation** The ATM25 network module hardware may be defective.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%IDTATM25-3-FAILTEARDOWNVC: Interface [chars], Failed to down vc [dec] (Cause: [chars])

**Explanation** The ATM25 network module hardware may be defective.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%IDTATM25-1-INITFAIL: IDTATM25([dec]/[dec]), Init failed, CSR[dec]=[hex].

**Explanation** The ATM25 network module hardware may be defective.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%IDTATM25-3-NOTIDTATM25: Device reported [hex]

**Explanation** The ATM25 network module hardware may be defective.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%IDTATM25-3-RXLOSTSYNC: IDB= [chars], RX lost sync, Interface reset

**Explanation** The Rx has hung.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%IDTATM25-3-TXHANG: IDB= [chars], TX hang, Interface reset

**Explanation** The Tx has hung.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%IDTATM25-6-TXLIMIT: ATM transmit bandwidth is limited to smallest shaped value.

**Explanation** The ATM transmit bandwidth is limited to the smallest shaped value. Any PVC configured with traffic shaping will limit the entire ATM interface to not exceed the bandwidth of any traffic shaped PVC.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message**

%IDTATM25-3-UNSUPPORTED: Interface [chars], [chars] not supported

**Explanation** The ATM25 network module hardware may be defective.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

## IF Messages

The following are Interface error messages.

**Error Message**

%IF-3-IDB\_LIST\_BAD\_REF\_COUNT: A bad reference count was encountered in an idb list element.

**Explanation** A software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.