



Configuring SNMP

This chapter describes how to configure Simple Network Management Protocol (SNMP) to query GSS devices for standard MIB resources.

It contains the following major sections:

- [Overview](#)
- [Supported MIBs and Notifications](#)
- [Configuring SNMP on the GSS](#)
- [Configuring SNMP Server Notifications](#)
- [Configuring the CPU Performance Threshold Values](#)
- [Configuring SNMP Server Trap Limits](#)
- [Specifying Recipients for SNMP Notification Operations](#)
- [Viewing the SNMP Status](#)
- [Viewing MIB Files on the GSS](#)

Overview

SNMP is a set of network management standards for IP-based internetworks. SNMP includes a protocol, a database-structure specification, and a set of management data objects. SNMP implementations typically consist of a management application running on one or more network management systems (NMSs), and agent applications, usually executing in firmware on various network devices.

SNMP obtains information from the network through a Management Information Base (MIB). The MIB is a database of code blocks called *MIB objects*. Each MIB object controls one specific function, such as counting how many bytes are transmitted through an agent's port. The MIB object consists of *MIB variables*, which define the MIB object name, description, and default value.

Each GSS or GSSM contains an SNMP agent, net-snmp version 5.1.2, that network management systems query for MIB resources. SNMP runs on GSS port 161 by default. The SNMP agent receives instructions from the SNMP manager and also sends management information back to the SNMP manager as events occur.

Supported MIBs and Notifications

Table 6-1 identifies the supported MIBs for the GSS.

Table 6-1 *SNMP MIB Support*

MIB Support	Capability MIB
CISCO-GSLB-DNS-MIB	CISCO-GSLB-DNS-CAPABILITY
Description: The GSS does not currently support any OIDs for this MIB, but it does support the related MIB SNMP traps (see Table 6-2).	
CISCO-GSLB-HEALTH-MON-MIB	CISCO-GSLB-HEALTH-MON-CAPABILITY
Description: The GSS does not currently support any OIDs for this MIB, but it does support the related MIB SNMP traps (see Table 6-2).	
CISCO-GSLB-SYSTEM-MIB	CISCO-GSLB-SYSTEM-CAPABILITY
Description: Defines the objects for network and system information of the GSLB as a network device. This MIB objects define information about GSLB status, GSLB peers (other GSLB devices on the same network that it interacts with) information and status, GSLB proximity information related statistics, and more. This MIB also defines the related notifications.	
CISCO-PROCESS-MIB	CISCO-PROCESS-CAPABILITY
Description: Defines the objects for monitoring CPU usage and active system processes. The CPU utilization MIBs provide aggregate CPU utilization for dual-code GSS devices.	

Table 6-1 *SNMP MIB Support*

MIB Support	Capability MIB
CISCO-SYSTEMS-EXT-MIB	CISCO-SYSTEM-EXT-CAPABILITY
Description: Monitors high availability (HA), SNMP SET errors, and bandwidths. This MIB also provides information about the core files that the GSS generates.	

The following URL provides details about the objects that the GSS supports for each MIB type:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

From this URL, choose the GSS from the Cisco Secure and VPN Products drop-down list and then click on the associated capability MIB.

In addition to the MIBs listed in [Table 6-1](#), the GSS supports the following generic MIBs:

- SNMPv2-MIB
- IF-MIB
- RFC1213-MIB
- IP-MIB
- TCP-MIB
- UDP-MIB
- HOST-RESOURCES-MIB (partially supported)
- UCD-SNMP-MIB (partially supported)

[Table 6-2](#) identifies the supported SNMP notifications (traps) for the GSS. The GSS generates the notifications only when you enable them using the GSS CLI (see the “[Configuring SNMP Server Notifications](#)” section).

Table 6-2 SNMP Trap Support

Notification Name	Notification Location
authenticationFailure	SNMPv2-MIB
Description: Indicates that the SNMP entity has received a protocol message that is not properly authenticated.	
coldStart	SNMPv2-MIB
Description: Indicates that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	
ciscoGslbAnswerEventStatusChange	CISCO-GSLB-DNS-MIB
Description: Indicates a change in the status of an answer element.	
ciscoGslbDnsEventClause	CISCO-GSLB-DNS-MIB
Description: Indicates when a transition occurs from the use of one clause to another for selecting an answer on a DNS rule match. For example, a transition occurs when a DNS rule uses a clause identified by the cgdSecondClauseId object instead of the cgdFirstClauseId object. The cgdFirstClauseId object contains the clause number used for selecting the most recent answer for a DNS rule. The cgdSecondClauseId object contains the clause number that was previously used to select an answer for the DNS rule	
ciscoGslbKalEventStatus	CISCO-GSLB-HEALTH-MON-MIB
Description: Indicates a change in the status of a keep alive associated with an answer element.	
ciscoGslbSystemPeerEventStatus	CISCO-GSLB-SYSTEM-MIB
Description: Indicates a change in the status of a GSS peer device. This notification is reported only by a GSS device with a cgsNodeService object value of "primary."	
cpmCPUFallingThreshold	CISCO-PROCESS-MIB
Description: Indicates when the CPU usage drops below the specified threshold.	
cpmCPURisingThreshold	CISCO-PROCESS-MIB
Description: Indicates when the CPU usage exceeds the specified threshold.	

Table 6-2 SNMP Trap Support

Notification Name	Notification Location
cseFailSwCoreNotifyExtended	CISCO-SYSTEM-EXT-MIB
Description: Indicates when the software becomes unresponsive and a core file is generated.	

Configuring SNMP on the GSS

Before you use SNMP to monitor the GSS or GSSM, you must enable the SNMP agent on each GSS device. In addition to enabling the SNMP agent on the GSS device, you also specify an SNMP community name, name of the contact person, and the physical location for the GSS device.



Note

Be aware that existing, pre-v2.0, SNMP community, contact, and location configurations are retained after a v3.0 software upgrade. For example, if you have configured a company contact in v1.3 and then upgrade to GSS v3.0, that contact will be retained after the v3.0 upgrade is completed.



Note

In the pre-v2.0 GSS software, a default community string is set to **public** after you enable SNMP. After a v2.0 software upgrade, however, no default community string is set when you enable SNMP.

You can add the **public** community string manually in the v2.0 software or higher as explained in the steps that follow. Any community strings that you configured in the pre-v2.0 GSS software will be retained after a v3.0 software upgrade.

Use the **snmp-server** command in global configuration mode to enable and configure SNMP on your GSS device.

To configure SNMP for a GSS device, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

If you are accessing the GSS remotely using Telnet or SSH, the CLI prompts you for the enable password. The default password is default. For more information about the enable password and configuring a new password, see the *Cisco Global Site Selector Getting Started Guide*.

2. Access global configuration mode.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Enable the SNMP agent by using the following command.

```
gss1.example.com(config)# snmp-server enable
```

4. Specify an SNMP community name for this GSS device by using the **snmp community-string** command. Each GSS device then becomes part of the named community. To change the SNMP community string, enter an unquoted text string with no space and a maximum length of 32 characters.

```
gss1.example.com(config)# snmp-server community-string public
```

5. Configure a contact for this GSS device using the **snmp-server contact** command. Enter an unquoted text string with a maximum of 255 characters without any spaces.

```
gss-pilot1.cisco.com(config)# snmp-server contact
JoeSmith-jsmith@cisco.com
```

6. Specify a location by using the **location** command and the *location* itself. The maximum length of the location is 255 characters.

```
gss1.example.com(config)# snmp-server location Boxborough
```

To disable SNMP or any of the parameters outlined above, use the **no** form of the **snmp** command. For example, to disable the SNMP contacts for the GSS, enter:

```
gss1.example.com(config)# no snmp-server contact
JoeSmith-jsmith@cisco.com
```

Configuring SNMP Server Notifications

You can enable traps on your GSS device by using the **snmp-server enable-traps** command in global configuration mode. To disable traps, use the **no** form of this command.

To configure SNMP server notifications for a GSS device, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

If you are accessing the GSS remotely using Telnet or SSH, the CLI prompts you for the enable password. The default password is default. For more information about the enable password and configuring a new password, see the *Cisco Global Site Selector Getting Started Guide*.

2. Access global configuration mode.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Enable the SNMP agent by using the following command:

```
gss1.example.com(config)# snmp-server enable
```

4. Enable SNMP server notifications by entering the **snmp-server enable-traps** command and following it with one of the available options:
 - **gslb**—Enables all SNMP GSLB notifications.
 - **gslb ans**—Enables SNMP GSLB answer-status change notifications only.
 - **gslb dns**—Enables SNMP GSLB DNS clause transition notifications only.
 - **gslb kal**—Enables SNMP GSLB keepalive-status change notifications only.
 - **gslb peer-status**—Enables SNMP GSLB peer-status change notifications only.
 - **core**—Enables SNMP core-file discovery notifications.
 - **performance**—Enables SNMP CPU usage rising and falling threshold notifications for monitoring CPU performance. By default, both of these threshold values are set to an average utilization rate of the 80 percent of the

total CPU utilization. To configure the CPU usage rising and falling threshold values, see the “[Configuring the CPU Performance Threshold Values](#)” section on page 6-9.

- **performance cpu-falling-threshold**—Enables only SNMP CPU usage falling threshold notification for monitoring CPU performance. By default, the threshold value is set to 80 percent of the total CPU utilization. To configure the CPU usage falling threshold value, see the “[Configuring the CPU Performance Threshold Values](#)” section on page 6-9.
- **performance cpu-rising-threshold**—Enables only SNMP CPU usage rising threshold notifications for monitoring CPU performance. By default, the threshold value is set to 80 percent of the total CPU utilization. To configure the CPU usage rising threshold value, see the “[Configuring the CPU Performance Threshold Values](#)” section on page 6-9.
- **snmp**—Enables all SNMP agent notifications.
- **snmp authentication**—Enables only SNMP agent authentication notifications.
- **snmp cold-start**—Enables only SNMP agent cold start notifications.

```
gss1.example.com(config)# snmp-server enable-traps kal
```

5. (SNMP v1 notifications only) Specify the GSS interface address associated with one of its Ethernet interfaces as the Agent-Address (trap source) to send in the trap. To specify the trap source, use the **snmp-server trap-source ethernet interface** command where the *interface* keyword specifies GSS interface 0 (the default) or 1.

```
gss1.example.com(config)# snmp-server trap-source ethernet 0
```

To disable SNMP server notifications, use the **no** form of the **snmp-server enable-traps** command. For example, to disable SNMP GSLB keepalive notifications, enter:

```
gss1.example.com(config)# no snmp-server enable-traps gslb kal
```

Configuring the CPU Performance Threshold Values

You can configure the GSS to issue SNMP traps that enable you to monitor CPU performance. The GSS can issue CPU performance notification traps when one or both of the following conditions exist:

- CPU usage rising—The GSS issues a CPU rising notification when the CPU usage exceeds the specified threshold. The GSS does not issue a second CPU rising threshold notification if the CPU usage remains above the usage rising threshold value for two consecutive monitoring intervals. The GSS issues another notification only after the CPU usage drops below the specified threshold value and then exceeds the threshold during subsequent monitoring intervals.
- CPU usage falling—The GSS issues a CPU falling notification when the CPU usage falls below the specified threshold. The GSS does not issue a second CPU falling threshold notification if the CPU usage remains below the usage falling threshold value for two consecutive monitoring intervals. The GSS issues another notification only after the CPU usage rises above the specified threshold value and then falls below the threshold during subsequent monitoring intervals.

The GSS monitors CPU usage every five seconds.

You can configure the CPU usage rising threshold value that determines when the GSS issues a CPU rising threshold crossing notification. Configure the rising threshold value by using the **snmp-server cpu-rising-threshold** command in global configuration mode.

The syntax of this command is as follows:

```
snmp-server cpu-rising-threshold rising_threshold
```

The *rising_threshold* argument is the threshold value as a percentage of the total CPU utilization. Enter a percentage value from 1 to 100. By default, the threshold value is set to 80 percent of the total CPU utilization. Use the **no** form of this command to return the threshold to its default value.

You can configure the CPU usage falling threshold value that determines when the GSS issues a CPU falling threshold crossing notification. Configure the falling threshold value using the **snmp-server cpu-falling-threshold** command in global configuration mode.

The syntax of this command is as follows:

```
snmp-server cpu-falling-threshold falling_threshold
```

The *falling_threshold* argument is the threshold value as a percentage of the total CPU utilization. Enter a percentage value from 1 to 100. By default, the threshold value is set to 80 percent of the total CPU utilization. Use the **no** form of this command to return the threshold to its default value.



Note

You must enable the SNMP performance trap type to enable the GSS to issue the CPU usage rising and falling threshold notifications (see the “[Configuring SNMP Server Notifications](#)” section on page 6-7).

To configure the CPU usage rising and falling threshold values, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable  
gss1.example.com#
```

If you are accessing the GSS remotely using Telnet or SSH, the CLI prompts you for the enable password. The default password is default. For more information about the enable password and configuring a new password, see the *Cisco Global Site Selector Getting Started Guide*.

2. Access global configuration mode.

```
gss1.example.com# config  
gss1.example.com(config)#
```

3. Enable the SNMP agent by using the following command:

```
gss1.example.com(config)# snmp-server enable
```

4. Enable the SNMP CPU performance notifications by using the following command:

```
gss1.example.com(config)# snmp-server enable-traps performance
```

5. Configure the CPU usage rising threshold value by using the following command:

```
gss1.example.com(config)# snmp-server cpu-rising-threshold 75
```

6. Configure the CPU usage falling threshold value by using the following command:

```
gss1.example.com(config)# snmp-server cpu-falling-threshold 75
```

To view the current CPU usage, use the **show processes | grep CPU** command. The command output displays the CPU usage as a percentage of the total CPU usage over a 5-second interval, 1-minute interval, and 5-minute interval.

Configuring SNMP Server Trap Limits

You can configure the maximum rate at which SNMP traps are set on your GSS device by using the **snmp-server trap-limit** command in global configuration mode. To set the default trap rate, use the **no** form of this command. The default is 25 traps per minute.

To configure SNMP server trap limits for a GSS device, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

If you are accessing the GSS remotely using Telnet or SSH, the CLI prompts you for the enable password. The default password is default. For more information about the enable password and configuring a new password, see the *Cisco Global Site Selector Getting Started Guide*.

2. Access global configuration mode.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Enable the SNMP agent by using the following command:

```
gss1.example.com(config)# snmp-server enable
```

4. Enable SNMP server trap limits by entering the **snmp-server trap-limit** command and following it with one of the available options and a specified value:

- **answer-trap value**—Configures a rate-limit for the answer trap.
- **dns-clause-trap value**—Configures the rate-limit for DNS clause traps.

- `keepalive-trap value`—Configures the rate-limit for the keepalive trap.

```
gss1.example.com(config)# snmp-server trap-limit answer trap 10
```

To set the trap rate back to its default rate, use the **no** form of the **snmp-server trap-limit** command as follows:

```
gss1.example.com(config)# no snmp-server trap-limit answer-trap
```

Specifying Recipients for SNMP Notification Operations

You can specify the recipient of an SNMP notification operation by using the **snmp-server host** command in global configuration mode. To remove the specified host, use the **no** form of this command.

To specify the recipient of an SNMP notification operation, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

If you are accessing the GSS remotely using Telnet or SSH, the CLI prompts you for the enable password. The default password is `default`. For more information about the enable password and configuring a new password, see the *Cisco Global Site Selector Getting Started Guide*.

2. Access global configuration mode.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Enable the SNMP agent by entering the following command:

```
gss1.example.com(config)# snmp-server enable
```

4. Specify the recipients of SNMP notification operations by using the **snmp-server host** command and a *host-address* and a *community-string*.

```
gss1.example.com(config)# snmp-server host 10.1.1.1 MyCommunity
```

5. Send SNMP traps to the specified host by entering the following command:

```
gss1.example.com(config)# snmp-server host 10.1.1.1 MyCommunity
traps
```

**Note**

You can configure a maximum of 10 hosts for traps notification.

6. Specify the version of the SNMP protocol used to send the traps by entering the **version** command and one of the available keywords:

- 1—Specifies SNMPv1 (the default).
- 2—Specifies SNMPv2c.

```
gss1.example.com(config)# snmp-server host 10.1.1.1 MyCommunity
traps version 2
```

7. Specify the host UDP port to use by entering the **udp-port** command and the port number.

```
gss1.example.com(config)# snmp-server host 10.1.1.1 MyCommunity
traps version 2 udp-port 500
```

To remove the recipient of an SNMP notification, use the **no** form of the **snmp-server host** command. For example, to disable all SNMP notifications for sample IP address 10.1.1.1, UDP port 100, enter:

```
gss1.example.com(config)# no snmp-server host 10.1.1.1 MyCommunity
traps version 2 udp-port 100
```

Viewing the SNMP Status

When SNMP is enabled, you can display the SNMP status on your GSS device by using the **show snmp** command.

The syntax of this command is as follows:

```
show snmp
```

Verify that your SNMP agent, net snmp agent version 5.1.2, is enabled or disabled, as well as the configured names of the community-string, location, and contact.

**Note**

You can also use the **show services** command to verify if SNMP is enabled or disabled.

You can also use the **show running-configuration** command to display the complete SNMP configuration.

For example, enter:

```

gss1.example.com# show snmp
SNMP is enabled
sys contact: JSmith jsmith@cisco.com
sys location: Boxborough

0 SNMP packets input
    0 Bad SNMP versions
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Trap PDUs

Community
-----
public

Host                               Port Version  Type
----                               -
16.1.1.11                          162  v2c        trap

Trap type                           Enabled
-----
GSLB KAL transition                 Yes
GSLB DNS clause change              Yes
GSLB answer transition              Yes
GSLB system core file discovery     Yes
GSLB system peer transition         Yes
SNMP authentication                 Yes
Cold Start                          Yes
Cpu Rising Threshold                 Yes
Cpu Falling Threshold                Yes

Trap type                           Threshold value
-----
Cpu Rising Threshold                 0
Cpu Falling Threshold                0

```

```

Trap type                               Trap Limit
-----
GSLB answer transition                  0
GSLB DNS clause change                  0
GSLB KAL transition                      0

gss1.example.com#

```

See the “[Configuring SNMP on the GSS](#)” section to change the status of your SNMP agent running on the GSS device.

Viewing MIB Files on the GSS

You can view the generic MIB files contained in the /mibs directory on the GSS by using the **dir** command. If you want to copy the MIB files from the /mibs directory on the GSS to another location on the GSS or to a remote network location, use the **scp** command.

For example, enter:

```

gss1.example.com# dir /mibs
total 1100
drwxr-xr-x  2 root  root   4096 Jul 18 08:45 .
drwxrwxrwx 19 root  root   4096 Jul 18 08:46 ..
-rw-r--r--  1 root  root  17455 Jul 18 08:45 AGENTX-MIB.txt
-rw-r--r--  1 root  root  19850 Jul 18 08:45 DISMAN-SCHEDULE-MIB.txt
-rw-r--r--  1 root  root  64311 Jul 18 08:45 DISMAN-SCRIPT-MIB.txt
-rw-r--r--  1 root  root  50054 Jul 18 08:45 EtherLike-MIB.txt
-rw-r--r--  1 root  root   4660 Jul 18 08:45 HCNUM-TC.txt
-rw-r--r--  1 root  root  52544 Jul 18 08:45 HOST-RESOURCES-MIB.txt
-rw-r--r--  1 root  root  10583 Jul 18 08:45 HOST-RESOURCES-TYPES.txt
-rw-r--r--  1 root  root   4015 Jul 18 08:45
IANA-ADDRESS-FAMILY-NUMBERS-MIB.txt
-rw-r--r--  1 root  root   4299 Jul 18 08:45 IANA-LANGUAGE-MIB.txt
-rw-r--r--  1 root  root  15661 Jul 18 08:45 IANAifType-MIB.txt
-rw-r--r--  1 root  root   5066 Jul 18 08:45 IF-INVERTED-STACK-MIB.txt
-rw-r--r--  1 root  root  71691 Jul 18 08:45 IF-MIB.txt
-rw-r--r--  1 root  root   6260 Jul 18 08:45 INET-ADDRESS-MIB.txt
-rw-r--r--  1 root  root  26781 Jul 18 08:45 IP-FORWARD-MIB.txt
-rw-r--r--  1 root  root  23499 Jul 18 08:45 IP-MIB.txt
-rw-r--r--  1 root  root  15936 Jul 18 08:45 IPV6-ICMP-MIB.txt
-rw-r--r--  1 root  root  48703 Jul 18 08:45 IPV6-MIB.txt
-rw-r--r--  1 root  root   2367 Jul 18 08:45 IPV6-TC.txt
-rw-r--r--  1 root  root   7257 Jul 18 08:45 IPV6-PCP-MIB.txt
-rw-r--r--  1 root  root   4400 Jul 18 08:45 IPV6-UDP-MIB.txt
-rw-r--r--  1 root  root   1174 Jul 18 08:45 RFC-1215.txt
-rw-r--r--  1 root  root   3067 Jul 18 08:45 RFC1155-SMI.txt
-rw-r--r--  1 root  root  79667 Jul 18 08:45 RFC1213-MIB.txt
-rw-r--r--  1 root  root  147822 Jul 18 08:45 RMON-MIB.txt
-rw-r--r--  1 root  root   4628 Jul 18 08:45 SMUX-MIB.txt
-rw-r--r--  1 root  root  15490 Jul 18 08:45 SNMP-COMMUNITY-MIB.txt

```

```

-rw-r--r-- 1 root  root  20750 Jul 18 08:45 SNMP-FRAMEWORK-MIB.txt
-rw-r--r-- 1 root  root   5261 Jul 18 08:45 SNMP-MPD-MIB.txt
-rw-r--r-- 1 root  root  19083 Jul 18 08:45 SNMP-NOTIFICATION-MIB.txt
-rw-r--r-- 1 root  root   8434 Jul 18 08:45 SNMP-PROXY-MIB.txt
-rw-r--r-- 1 root  root  21495 Jul 18 08:45 SNMP-TARGET-MIB.txt
-rw-r--r-- 1 root  root  38035 Jul 18 08:45 SNMP-USER-BASED-SM-MIB.txt
-rw-r--r-- 1 root  root  33430 Jul 18 08:45 SNMP-VIEW-BASED-ACM-MIB.txt
-rw-r--r-- 1 root  root   8263 Jul 18 08:45 SNMPv2-CONF.txt
-rw-r--r-- 1 root  root  25052 Jul 18 08:45 SNMPv2-MIB.txt
-rw-r--r-- 1 root  root   8924 Jul 18 08:45 SNMPv2-SMI.txt
-rw-r--r-- 1 root  root  38034 Jul 18 08:45 SNMPv2-TC.txt
-rw-r--r-- 1 root  root   3981 Jul 18 08:45 SNMPv2-TM.txt
-rw-r--r-- 1 root  root  10765 Jul 18 08:45 TCP-MIB.txt
-rw-r--r-- 1 root  root   2058 Jul 18 08:45 UCD-DEMO-MIB.txt
-rw-r--r-- 1 root  root   3131 Jul 18 08:45 UCD-DISKIO-MIB.txt
-rw-r--r-- 1 root  root   2928 Jul 18 08:45 UCD-DLMOD-MIB.txt
-rw-r--r-- 1 root  root   8037 Jul 18 08:45 UCD-IPFWACC-MIB.txt
-rw-r--r-- 1 root  root  30343 Jul 18 08:45 UCD-SNMP-MIB.txt
-rw-r--r-- 1 root  root   4076 Jul 18 08:45 UDP-MIB.txt

```