

10 SNMP (Simple Network Management Protocol)

Introduction

The Simple Network Management Protocol (SNMP) is an application layer protocol that allows network devices to exchange management information. SNMP works by sending messages, called protocol data units (PDUs), to network devices. Network administrators use SNMP to monitor network performance and to solve network problems.

An SNMP managed network is comprised of three fundamental parts: agents, managed devices, and network management systems (NMSs). An agent, which resides within a managed device (i.e., a switch), is responsible for translating its local knowledge of management information into a form compatible with SNMP. When certain defined asynchronous events occur within a switch, the managed device sends traps, in the form of SNMP, to a designated NMS. The NMS then views and monitors the switch's information through management software applications such as HP Open View, X-Vision, or WebView.

SNMP parameters and traps are configurable through the **snmpc** command. For more information on this command, refer to *Configuring SNMP Parameters and Traps* on page 10-2. Additionally, you can view SNMP statistics through the **snmps** command. For more information on this command, refer to *Viewing SNMP Statistics* on page 10-7. Both of these commands are also listed on the **Networking** menu.

Configuring SNMP Parameters and Traps

The **snmpc** command allows you to configure SNMP parameters and set traps that will be sent to network management stations. The **snmpc** command also enables you to add, modify, or delete SNMP parameters. The **snmpc** command is listed on the **Networking** menu. For more information about the networking menu, see Chapter 22, “IP Routing.” To configure SNMP parameters, enter the following command:

snmpc

A screen similar to the following displays:

SNMP current configuration:

- 1) **Set Community Name** - public
- 2) **Get Community Name** - public
- 3) **Trap Community Name** - public
- 4) **Broadcast Traps** - disabled
- 5) **0 Unicast Traps** - disabled

(save/quit/cancel)

:

- To change a value, enter the number corresponding to that value, an (=), and the new value. For example, to enable broadcast traps, enter **4=enabled**.
- To clear an entry, specify the value as (.), as in **2=.** Note that true/false values and enabled/disabled values cannot be cleared.
- To save all your modifications, enter **save**.
- To cancel all your modifications, enter **Cancel** or **Ctrl-C**
- To view the parameters currently configured, enter **?**

1) Set Community Name

The Set Community Name (up to 16 characters) is a password that enables NMS stations to read and write objects through SNMP. The default Set Community Name is “public,” which allows all NMS stations read and write access to read-write objects. If you want to specify a Set Community name, enter a **1**, an equal sign (=), and the new Set Community Name. The following is an example display:

1=alpha

Note: Set Community Names with spaces must be enclosed in quotations (e.g., “**test lab**”).

2) Get Community Name

The Get Community Name (up to 16 characters) is a password that enables NMS stations to read objects defined in the MIBs. The default Get Community Name is “public,” which allows all NMS station read access to readable objects. If you want to specify a Get Community Name, enter a **2**, an equal sign (=), and the new Get Community Name. The following is an example display:

2=beta

Note: Get Community Names with spaces must be enclosed in quotations (e.g., “**data center**”).

3) Trap Community Name

The Trap Community Name (up to 16 characters) is a password that enables NMS stations to collect traps (provided the NMS stations are configured with the same corresponding Trap Community Name). The default Trap Community Name is “public,” which allows the switch to send traps to all NMS stations configured with the Trap Community Name, “public.” If you want to specify a Trap Community Name, enter a **3**, an equal sign (**=**), and the new Trap Community Name. The following is an example display.

3=trap1

Note: Trap Community Names with spaces must be enclosed in quotations (e.g., “**trap 1**”).

4) Broadcast Traps

When broadcast traps are enabled, the switch transmits traps to all NMSs in the default group. If you enable this parameter, unicast traps (see option 5 below) will automatically be disabled. The default for broadcast traps is **disabled**. To enable broadcast traps, enter the following command:

4=enabled

The following prompt displays:

UDP destination port (162):

Enter the UDP (User datagram protocol) destination port for the traps. UDP port 162 is the default port and is commonly used for traps; however, the destination port can be re-defined to accommodate a network management station using a nonstandard port.

Note: The destination port configured here must correspond to the UDP destination port configured at the receiving network management station(s).

5) Unicast Traps

When unicast traps are enabled, the switch transmit traps only to the IP address(es) defined in the **snmpc** list. If you enable this parameter, broadcast traps (see option 4 above) will automatically be disabled. The default for unicast traps is disabled. To enable unicast traps, enter the following command:

5=enabled

Note

If both broadcast and unicast traps are disabled, then the switch does not transmit any traps.

Procedure for Defining a New Network Management Station

- a. To define a new network management station, enter 6, followed by an equal sign (=), and the IP address of the network management station to receive traps. You can define up to a maximum of ten network management stations (15 is the last number you can use to define the tenth trap). If there are network management stations already defined in this menu, you can add more stations by using any number above the highest existing station. The following is an example of how to define the first network management station:

6=123.12.1.1

- b. The following prompt displays:

Enter trap mask words 0:1 (ffffff:ffffff):

The mask value **ffffff:ffffff** indicates that all traps are enabled for words 0 and 1. If you want to accept this default, simply press <Enter>. If you want to set one or more specific traps for words 0 and 1, you must calculate the bit configurations and enter the new mask value at the prompt. Trap types and their bit positions are listed in the tables beginning on page 10-10. Displayed below is a sample configuration for setting a combination of traps.

Bit Configurations for Setting Traps

word 0 (4 bytes)

00 00 00 00

↑

bit 0

:

word 1 (4 bytes)

00 00 00 00

↑

bit 0

You would then enter the the final mask value of the traps, as follows:

Enter trap mask words 0:1 (ffffff:ffffff): 0000C001:00000200

- c. The following prompt displays:

Enter trap mask words 2:3 (ffffff:ffffff):

Enter the trap type(s) for words 2 and 3. If you want to accept the default (all traps enabled for words 2 and 3), press <Enter>. To set one or more specific traps, again calculate the bit configurations and enter the new mask value at the prompt.

- d. The following prompt displays:

Enter destination port (162):

Enter the UDP destination port for the traps configured above. If you choose the default, port 162, simply press **<Enter>** at the prompt.

- e. The following prompt displays:

NMS state (on):

Indicate whether or not traps will be sent to this Network Management Station (the NMS defined in step a). If the NMS state is enabled (**on**), the NMS will be notified of traps. Simply press **<Enter>** to accept the default (**on**). If the NMS state is disabled (**off**), the NMS will not be notified of traps.

- f. The following prompt displays:

Special Access? (no): yes

Select whether or not this Network Management Station has special access. If you enter **yes**, this NMS will have administrative privileges such as modifying, deleting, or adding to other trap entries as well as its own. Without special access, an NMS can only update its own entry. If you choose the default, **no**, simply press **<Enter>** at the prompt.

- g. After you have saved your configuration, the prompt re-displays. The above entries will create an NMS number 6 in the list. Traps will be sent to the IP address specified for that NMS station (provided the NMS state is **on** and unicast traps are **enabled**). To view your new SNMP configuration, again enter the **snmpc** command. The following is a sample display of the output from the **snmpc** command after the above sample configuration:

SNMP current configuration:

```

1) Set Community Name   - admin
2) Get Community Name   - public
3) Trap Community Name  - trap1
4) Broadcast Traps      - disabled
5) 1 Unicast Traps      - enabled
6) NMS IP address       - 123.12.1.1           /162 --bfffffff:ffffff (on) (SA)
                                           -- ffffffff:ffffff
(save/quit/cancel)
:
```

The values that appear to the immediate right of the NMS IP address are: the UDP destination port number (**162**), the trap bit masks (**fffffff:ffffff**), the functional state of the NMS (**on**), and the special access (**SA**) status (this does not appear if you selected **no** for special access in step 12 above). To add network management stations to this current SNMP configuration, enter the next highest entry number from the last defined NMS. For example, if you wanted to add another NMS to the above sample configuration, you would enter the following:

7=123.22.2.2

Configuring SNMP Parameters and Traps

Please note that any additional NMS entries must have a new IP address. Repeat steps 2 through 6 to continue configuring additional NMS entries. Once you save your configuration and re-enter the **snmpc** command at the prompt, the screen refreshes to include the new NMS entry. The following is a sample display:

SNMP current configuration:

```
1) Set Community Name - public
2) Get Community Name - public
3) Trap Community Name - public
4) Broadcast Traps    - disabled
5) 1 Unicast Traps   - enabled
6) NMS IP address     - 123.12.1.1      /162 -- ffffffff:bfffffff (on) (SA
                                         -- ffffffff:ffffffff)
7) NMS IP address     - 123.22.2.2      /162 -- ffffffff:ffffffff (on)
                                         -- ffffffff:ffffffff
(save/quit/cancel)
:
```

Viewing SNMP Statistics

The **snmps** command is used to display SNMP statistics. The command displays the SNMP activities since the last time the switch was powered on, or since the last Reset was executed. Also displayed is a list of the current traps.

The **snmps** command is listed on the **Networking** menu. For more information about the networking menu, see Chapter 22, “IP Routing.” To display SNMP statistics, enter the following command:

```
snmps
```

A screen similar to the following displays:

SNMP Statistics		
	In	Out
Total Packets	67	67
Bad Versions	0	
Bad Community Names	0	
Bad Community Use	0	
Bad Type Discards:	0	
ASN Parse Errors	0	
Too Big Errors	0	0
No Such Name Errors	0	1
Bad Value Errors	0	0
Read Only Errors	0	0
General Errors	0	0
Total Variable Requests	186	
Total Set Variable Requests	0	
Get Requests	17	0
Get Next Requests	50	0
Set Requests	0	0
Get Responses	0	67
Authentication Trap Enables:	0	
Traps	0	0

Trap generation is ENABLED to these management stations:

```
198.206.1.1 /162 -- ffffffff:bfffffff (on)
198.2.1.1   /162 -- ffffffff:7fffffff (off) (SA)
```

Total Packets

The total number of packets received and sent.

Bad Version

The total number of SNMP messages delivered to the switch SNMP protocol entity that were for an unsupported SNMP version.

Bad Community Names

The total number of SNMP message names delivered to the switch SNMP protocol entity that used an unknown SNMP community name.

Bad Community Use

The total number of SNMP messages delivered to the SNMP protocol entity which represented an SNMP operation that was not allowed by the SNMP community named in the message.

Bad Type Discards

The total number of SNMP entries that were discarded because the request type was not recognized.

ASN Parse Errors

The total number of ASN.1 or BER errors encountered by the SNMP protocols entity when decoding received SNMP Messages.

Too Big Errors

The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'tooBig'.

No Such Name Error

The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'noSuchName'.

Bad Value Errors

The total number of valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'readOnly.' It is a protocol error to generate an SNMP PDU which contains the value 'readOnly' in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.

Read Only Errors

The total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is 'Read Only'.

General Errors

The total number of SNMP PDUs delivered to the OmniAccess 512 SNMP protocol entity and for which the value of the errors-status field is 'GenError'.

Total Variable Requests

The total number of MIB objects which Requests have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

Total Set Variable Requests

The total number of MIB objects which Requests have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.

Get Requests

The total number of SNMP Get-Request PDUs which have been accepted and processed by the OmniAccess 512 SNMP protocol entity.

Get Next Requests

The total number of SNMP Get-Next PDUs which have been accepted and processed by the OmniAccess 512 SNMP protocol entity.

Set Requests

The total number of SNMP Set-Request Requests Accepted PDUs which have been accepted and processed by the OmniAccess 512 SNMP protocol entity.

Get Responses

The total number of SNMP Response PDUs which have been accepted and processed by the OmniAccess 512 SNMP protocol entity.

Authentication Trap Enables

Indicates whether the SNMP agent Enable process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information, providing a means to enable all authentication-failure traps.

Traps

The number of SNMP Trap PDUs that have been generated by the SNMP protocol entity. Traps are broadcast only.

Traps are broadcast only

This appears if traps are set to broadcast. The address is the broadcast address of the default VLAN of AutoTracker group 1.

Trap generation is ENABLED to these management stations

This appears if you have used the **snmpc** command to set up one or more management stations to receive traps. The trap tables on the following page list the traps that are currently supported.

Trap Tables

The tables on the following pages provide the following information on traps:

Trap. The object name of the trap as it is defined in the corresponding MIB (Management Information Base). Alcatel supports standardized and proprietary MIBS.

Object ID. The SNMP object identifier (OID) for this trap.

Description. A brief explanation describing the circumstances under which a specific trap is generated.

Bit Position. The trap's specific position in a bit mask (a bit mask is a binary notation which represents a combination of all four trap words). By mapping a specific trap to its binary position, you can determine whether or not a trap is enabled. For example, a trap is enabled if its corresponding bit is set to 1 and disabled if its corresponding bit is set to 0.

Word. A word is a set of four consecutive bytes within a system's memory. Alcatel allocates a total of four words for trap representation. Each of the 32 bit positions within a word corresponds to a specific trap. The first word, Word 0, contains only standard traps as they are defined within RFC (MIB) documents. Words 1, 2, and 3 contain Alcatel-specific traps.

Hex Value. The resulting hexadecimal value of the bit mask.

Trap Text and Variable Description. A trap text is a brief statement containing additional information that can help you narrow down the source of the trap, such as slot/port numbers, module types, and MAC addresses (variable descriptions have been added for your convenience). When a specific trap is triggered, it may display in various text formats, depending on the software application through which it is viewed. The trap texts in the following tables are examples of trap texts displayed through the HP OpenView Alarm Log and the Traps window in X-Vision Discovery. Traps can also be viewed through X-WebVision. For more information on these NMS applications, see the on-line documentation.

SNMP Standard Traps

This section lists the standard traps that are defined within RFC (MIB) documents. These traps signify events as they occur on common network devices.

Trap	coldStart
Object ID	1.3.6.1.2.1.11.0
Description	The sending protocol entity is re-initializing itself such that the agent's configuration or the protocol entity implementation may be altered.
Bit Position (Word 0)	0
Hex Value (Word 0)	1
Trap Text and Variable Descriptions	Cold Start

Trap	warmStart
Object ID	1.3.6.1.2.1.11.1
Description	The sending protocol entity is re-initializing itself such that neither the agent's configuration nor the protocol entity implementation may be altered.
Bit Position (Word 0)	1
Hex Value (Word 0)	2
Trap Text and Variable Descriptions	Warm Start

Trap	linkDown
Object ID	1.3.6.1.2.1.11.2
Description	The sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.
Bit Position (Word 0)	2
Hex Value (Word 0)	4
Trap Text and Variable Descriptions	<div data-bbox="393 1365 972 1434" data-label="Text"> <p>Link Down (port 1)</p> </div> <div data-bbox="475 1488 846 1568" data-label="Text"> <p>Port Index. The port number which identifies the failed communication link.</p> </div>

Trap	linkUp
Object ID	1.3.6.1.2.1.11.3
Description	The sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.
Bit Position (Word 0)	3
Hex Value (Word 0)	8
Trap Text and Variable Descriptions	<div data-bbox="393 690 972 758">Link Up (port 1)</div> <p>Port Index. The port number which identifies where the communication link has come up.</p>

Trap	authenticationFailure
Object ID	1.3.6.1.2.1.11.4
Description	The sending protocol entity is the addressee of a protocol message that is not properly authenticated.
Bit Position (Word 0)	4
Hex Value (Word 0)	10
Trap Text and Variable Descriptions	Authentication Failure

Trap	egpNeighborLoss
Object ID	1.3.6.1.2.1.11.5
Description	An EGP neighbor for whom the sending protocol entity was an EGP peer has been marked down and the peer relationship no longer exists.
Bit Position (Word 0)	5
Hex Value (Word 0)	20
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;">Neighbor Loss (neigh addr 192.168.10.1)</div> <p style="margin-left: 400px;">Neighbor IP Address. The IP address of this entry's EGP neighbor.</p>

Trap Type	newRoot
Object ID	1.3.6.1.2.1.17.0.1
Description	Sent by a bridge that became the new root of the Spanning Tree.
Bit Position (Word 0)	10
Hex Value (Word 0)	400
Trap Text and Variable Descriptions	Spanning Tree: A new agent has become the root of the Spanning Tree.

<i>Trap</i>	topologyChange
<i>Object ID</i>	1.3.6.1.2.1.17.0.2
<i>Description</i>	A bridge's configured ports either transitioned from Learning state to Forwarding state or from Forwarding state to Blocking state. This trap will not be sent if a newRoot trap was sent for the same transition.
<i>Bit Position (Word 0)</i>	11
<i>Hex Value (Word 0)</i>	800
<i>Trap Text and Variable Descriptions</i>	Spanning Tree: A configured port's state has transitioned.

Trap	risingAlarm
Object ID	1.3.6.1.2.1.16.0.1
Description	The value of an Ethernet statistical variable (i.e., a member of the Ethernet statistics group as defined by RFC 1757) has exceeded its rising threshold. The variable's rising threshold and whether it will generate an SNMP trap for this condition are configured by a network management station running RMON.
Bit Position (Word 0)	14
Hex Value (Word 0)	4000
Trap Text and Variable Descriptions	<div> <p>Variable. The MIB object identifier for the variable being sampled.</p> </div> <div> <p>Alarm index. An index value for this entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device.</p> </div> <div> <p>An RMON alarm entry crossed its rising threshold (index 25 var 2 type 1 value 201 rising threshold 200)</p> </div> <div> <p>Value. The value of the statistic during the last sampling period. For example, if the sample method is Delta Value, this value will be the difference between the samples at the beginning and end of the period. If the sample method is Absolute Value, this value will be the sampled value at the end of the period. This is the value that is compared with the rising threshold.</p> </div> <div> <p>Sampling method. The method of sampling the selected variable and calculating the value for comparison with the thresholds. Possible values are integers 1 and 2:</p> <ol style="list-style-type: none"> 1 Absolute Value. The value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. 2 Delta Value. The value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds. </div> <div> <p>Rising Threshold. A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, this trap is generated. After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the Falling Threshold value.</p> </div>

Trap	fallingAlarm
Object ID	1.3.6.1.2.1.16.0.2
Description	The value of an Ethernet statistical variable (i.e., a member of the Ethernet statistics group as defined by RFC 1757) has dipped below its falling threshold. The variable's falling threshold and whether it will generate an SNMP trap for this condition are configured by a network management station running RMON.
Bit Position (Word 0)	15
Hex Value (Word 0)	8000
Trap Text and Variable Descriptions	<div> <div> <p>Variable. The MIB object identifier for the variable being sampled.</p> </div> <div> <p>Alarm index. An index value for this entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device.</p> </div> </div> <div> <p>An RMON alarm entry crossed its falling threshold (index 25 var 2 type 1 value 100 falling threshold 9)</p> </div> <div> <p>Value. The value of the statistic during the last sampling period. For example, if the sample method is Delta Value, this value will be the difference between the samples at the beginning and end of the period. If the sample method is Absolute Value, this value will be the sampled value at the end of the period. This is the value that is compared with the falling threshold.</p> <p>Falling Threshold. A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was more than this threshold, this trap is generated.</p> <p>After a falling event is generated, another such event will not be generated until the sampled value falls above this threshold and reaches the Rising Threshold value.</p> </div> <div> <p>Sampling method. The method of sampling the selected variable and calculating the value for comparison with the thresholds. Possible values are:</p> <ol style="list-style-type: none"> 1 Absolute Value. The value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. 2 Delta Value. The value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds. </div>

Trap Type	dsx3LineStatusChange
Object ID	1.3.6.1.2.1.10.30.15.0.1
Description	The value of an instance dsx3LineStatus changed.
Bit Position (Word 0)	16
Hex Value (Word 1)	1 0000
Trap Text and Variable Descriptions	<div><div>Line Status Change (line status 1, last change 4)</div><div><div>DSX3 Line Status. The line status of the interface. It contains loopback, failure, received alarm, and transmitted alarm information. Valid values range from 1 to 8191.</div><div>Last Change. The last value of MIB II's sysUpTime object at the time this DS3 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this value is zero .</div></div></div>

Trap	dsx1LineStatusChange
Object ID	1.3.6.1.2.1.10.18.15.0.1
Description	The value of an instance dsx1LineStatus changed.
Bit Position (Word 0)	17
Hex Value (Word 1)	2 0000
Trap Text and Variable Descriptions	<div> <div>Line Status Change (line status 1, last change 2)</div> <div> <p>DSX1 Line Status. The line status of the interface. It contains loopback, failure, received alarm, and transmitted alarm information. Valid values range from 1 to 8191.</p> <p>Last Change. The last value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this value is zero .</p> </div> </div>

Extended Traps

This section lists Alcatel-specific traps. These extended traps are generated specifically by Alcatel switch devices.

Trap Type	tempAlarm
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.1
Description	The temperature sensor(s) have detected a temperature in the chassis that exceeds the threshold. These sensors are physically located on the MPM module, but can detect temperature changes throughout the chassis.
Bit Position (Word 1)	0
Hex Value (Word 1)	1
Trap Text and Variable Descriptions	Temperature Sensor has changed state to Over Threshold

Trap Tables

<i>Trap Type</i>	moduleChange
<i>Object ID</i>	1.3.6.1.4.1.800.3.1.1.4.0.2
<i>Description</i>	A module was either inserted or removed from the chassis. In some cases, this trap may also be generated when a module is reset.
<i>Bit Position (Word 1)</i>	1
<i>Hex Value (Word 1)</i>	2

<p>Trap Text and Variable Descriptions</p>	<div data-bbox="397 237 1320 296" style="background-color: #cccccc; padding: 5px; border: 1px solid black; text-align: center;"> Module was inserted or removed from chassis (slot 4, subunit 1, type 10) </div> <p>Slot number. The slot number on the front of the chassis where this module was inserted or removed.</p> <p>Submodule Type. Indicates the submodule that was inserted or removed. Typically this value will be 1, meaning the base module was inserted or removed. If this value is 2, then HSM module 1 was moved. If this value is 3, then HSM module 2 was moved.</p> <p>Module Type. Indicates the module type that was inserted or removed. The following integers are valid values:</p> <ul style="list-style-type: none"> 4 HSM 5 MPM 6 ESM 8-port 10BASE-T 7 ESM 16-port 8 TSM 6-port UTP/STP 9 FSM FDDI module 10 FSM CDDI module 11 ESM 4-port 12 ASM .5 MB multi-mode 13 ESM 12-port 10BASE-T 14 ESM 6-port universal module 15 MPM version II 16 ATM DS-3 17 FSM FDDI single mode 18 ASM .5 MB single mode 19 ASM UTP 20 ESM 8-port fiber 21 ESM 12-port Telco 22 TSM fiber 23 ASM 2 MB multi-mode 24 ASM 2 MB single mode 25 WSM 26 WSM BRI 27 HSM2 base slot type 28 PizzaSwitch reserved 29 TSM CD-6 30 ASM 2 MB single mode 33 10Meg Ether Universal 34 ATM E3 (European) 35 Ether 100 FX Sngl Full Dup 36 Ether 100 FX Multi Full Dup 37 Ether 100 TX CU Full Dup 39 PizzaPort (repeater)
---	--

Trap Type	powerEvent
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.3
Description	A power supply was either inserted or removed from the chassis, or there is a problem with the power supply. This trap is also generated when a power supply is switched on or off.
Bit Position (Word 1)	2
Hex Value (Word 1)	4
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Power Supply was inserted or removed from chassis or has a problem (ps1 3, ps2 2) </div> <p>Power Supply Status. The current state of power supply 1 (ps1) and power supply 2 (ps2). The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Unknown 2 No power supply is present 3 Power supply is okay. 4 Power supply is bad.

Trap Type	controllerEvent
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.4
Description	A chassis controller (MPM) lost or gained the state of the master.
Bit Position (Word 1)	3
Hex Value (Word 1)	8
Trap Text and Variable Descriptions	<div>Chassis controller (MPM) lost or gained master control (slot 1, state 3)</div> <p>Slot. The slot number of the MPM that has lost or gained master control. Valid values are:</p> <ul style="list-style-type: none">1 Slot Number 12 Slot Number 2 <p>State. The current state of the MPM in the slot. The following integers are valid values:</p> <ul style="list-style-type: none">1 Unknown2 Invalid3 Master4 Slave

Trap Type	loginViolation
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.5
Description	A login attempt for the User Interface (UI) failed due to an incorrect login ID or an invalid password. Three (3) consecutive unsuccessful attempts will trigger this alarm.
Bit Position (Word 1)	4
Hex Value (Word 1)	10
Trap Text and Variable Descriptions	Login Attempt failed due to invalid ID or password.

Trap Type	macVlanViolation
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.6
Description	Data from a MAC address that previously came from one port is now coming from another port. The new port is in a different Group (port-based VLAN) than the previous port.
Bit Position (Word 1)	5
Hex Value (Word 1)	20
Trap Text and Variable Descriptions	<div>Receiving Port VLAN ID has changed (bridge address 0036589adf01)</div> <p>MAC Address. The MAC address from which data has come from two different ports in two different groups.</p>

Trap Type	macDuplicatePort
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.7
Description	Data from a MAC address that previously came from one port is now coming from another port. The new port is in the same Group (port-based VLAN) as the previous port.
Bit Position (Word 1)	6
Hex Value (Word 1)	40
Trap Text and Variable Descriptions	<div>VLAN Receiving Port has changed (bridge address 00145221cd02)</div> <p>MAC Address. The MAC address from which data has come from two different ports in the same group.</p>

Trap Type	portLinkUpEvent																																												
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.8																																												
Description	A physical, logical, or virtual port was enabled. These ports may be enabled through the UI or Switch Manager. Note that if you enable a physical port, any associated logical and virtual ports will also be enabled. And if you enable a logical port, such as an ATM service, associated virtual ports will be enabled.																																												
Bit Position (Word 1)	7																																												
Hex Value (Word 1)	80																																												
Trap Text and Variable Descriptions	<div>Physical, logical or virtual port was enabled (slot 2 IF 2 type 203 instance 1)</div> <div> <p>Slot number. The slot number for the module that contains this port.</p> <p>Port number. The port number on this module that was enabled.</p> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <table> <tr><td>1</td><td>Unknown</td></tr> <tr><td>2</td><td>Other</td></tr> <tr><td>3</td><td>Router</td></tr> <tr><td>4</td><td>Bridge</td></tr> <tr><td>5</td><td>Trunk</td></tr> <tr><td>6</td><td>ATM trunk port</td></tr> <tr><td>7</td><td>ATM LAN Emulation port</td></tr> <tr><td>8</td><td>Classical IP</td></tr> <tr><td>9</td><td>ATM MUX</td></tr> <tr><td>203</td><td>Ethernet 10BASE-T</td></tr> <tr><td>204</td><td>Ethernet 100BASE-T</td></tr> <tr><td>205</td><td>Token Ring 4 mbs</td></tr> <tr><td>206</td><td>Token Ring 16 mbs</td></tr> <tr><td>207</td><td>FDDI</td></tr> <tr><td>208</td><td>CDDI</td></tr> <tr><td>209</td><td>ATM 25 mbs</td></tr> <tr><td>210</td><td>ATM 50 mbs</td></tr> <tr><td>211</td><td>DS-1</td></tr> <tr><td>212</td><td>DS-3</td></tr> <tr><td>213</td><td>OC-3</td></tr> <tr><td>214</td><td>OC-12</td></tr> <tr><td>215</td><td>OC-48</td></tr> </table> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p> </div>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

Trap Type	portLinkDownEvent																																												
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.9																																												
Description	A physical, logical, or virtual port was disabled. These ports may be disabled through the UI or Switch Manager. Note that if you disable a physical port, any associated logical and virtual ports will also be disabled. And if you disable a logical port, such as an ATM service, associated virtual ports will also be disabled.																																												
Bit Position (Word 1)	8																																												
Hex Value (Word 1)	100																																												
Trap Text and Variable Descriptions	<div>Physical, logical or virtual port was disabled (slot 2 IF 2 type 203 instance 1)</div> <p>Slot number. The slot number for the module that contains this port.</p> <p>Port number. The port number on this module that was disabled.</p> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <table> <tr><td>1</td><td>Unknown</td></tr> <tr><td>2</td><td>Other</td></tr> <tr><td>3</td><td>Router</td></tr> <tr><td>4</td><td>Bridge</td></tr> <tr><td>5</td><td>Trunk</td></tr> <tr><td>6</td><td>ATM trunk port</td></tr> <tr><td>7</td><td>ATM LAN Emulation port</td></tr> <tr><td>8</td><td>Classical IP</td></tr> <tr><td>9</td><td>ATM MUX</td></tr> <tr><td>203</td><td>Ethernet 10BASE-T</td></tr> <tr><td>204</td><td>Ethernet 100BASE-T</td></tr> <tr><td>205</td><td>Token Ring 4 mbs</td></tr> <tr><td>206</td><td>Token Ring 16 mbs</td></tr> <tr><td>207</td><td>FDDI</td></tr> <tr><td>208</td><td>CDDI</td></tr> <tr><td>209</td><td>ATM 25 mbs</td></tr> <tr><td>210</td><td>ATM 50 mbs</td></tr> <tr><td>211</td><td>DS-1</td></tr> <tr><td>212</td><td>DS-3</td></tr> <tr><td>213</td><td>OC-3</td></tr> <tr><td>214</td><td>OC-12</td></tr> <tr><td>215</td><td>OC-48</td></tr> </table> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

<i>Trap Type</i>	portPartitioned
<i>Object ID</i>	1.3.6.1.4.1.800.3.1.1.4.0.10
<i>Description</i>	The physical port detected jabber (i.e., the port has transitioned through enable/disable states more than 50 times in the past 200 ms). Jabber may be produced by a bad port connection, such as a faulty cable.
<i>Bit Position (Word 1)</i>	9
<i>Hex Value (Word 1)</i>	200

Trap Text and Variable Descriptions	<div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; text-align: center; margin-bottom: 10px;"> Port jabber detected (enabled/disabled faster than 50 times in 200 ms) (slot 2, IF 2, type 203, instance 1) </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Slot number. The slot number for the module that contains this port.</p> <p>Port number. The port number on this module that detected jabber.</p> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 5%;">1</td><td>Unknown</td></tr> <tr><td>2</td><td>Other</td></tr> <tr><td>3</td><td>Router</td></tr> <tr><td>4</td><td>Bridge</td></tr> <tr><td>5</td><td>Trunk</td></tr> <tr><td>6</td><td>ATM trunk port</td></tr> <tr><td>7</td><td>ATM LAN Emulation port</td></tr> <tr><td>8</td><td>Classical IP</td></tr> <tr><td>9</td><td>ATM MUX</td></tr> <tr><td>203</td><td>Ethernet 10BASE-T</td></tr> <tr><td>204</td><td>Ethernet 100BASE-T</td></tr> <tr><td>205</td><td>Token Ring 4 mbs</td></tr> <tr><td>206</td><td>Token Ring 16 mbs</td></tr> <tr><td>207</td><td>FDDI</td></tr> <tr><td>208</td><td>CDDI</td></tr> <tr><td>209</td><td>ATM 25 mbs</td></tr> <tr><td>210</td><td>ATM 50 mbs</td></tr> <tr><td>211</td><td>DS-1</td></tr> <tr><td>212</td><td>DS-3</td></tr> <tr><td>213</td><td>OC-3</td></tr> <tr><td>214</td><td>OC-12</td></tr> <tr><td>215</td><td>OC-48</td></tr> </table> </div> <div style="width: 45%;"> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p> </div> </div>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

Trap Type	portRecordMismatch
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.11
Description	The port configuration is different from the previous configuration. Typically this trap is generated when a NIC of one type is swapped for a different type (i.e., Ethernet for FDDI, ATM for Token Ring, etc.).
Bit Position (Word 1)	10

Hex Value (Word 1)	400																																												
Trap Text and Variable Descriptions	<div>Port configuration different than previously detected (slot 2, IF 2, type 203, instance 1)</div> <div><p>Slot number. The slot number for the module that contains this port.</p><p>Port number. The port number on this module that has a different configuration.</p><p>Port Type. The physical type of this port. The following integers are valid values:</p><table><tr><td>1</td><td>Unknown</td></tr><tr><td>2</td><td>Other</td></tr><tr><td>3</td><td>Router</td></tr><tr><td>4</td><td>Bridge</td></tr><tr><td>5</td><td>Trunk</td></tr><tr><td>6</td><td>ATM trunk port</td></tr><tr><td>7</td><td>ATM LAN Emulation port</td></tr><tr><td>8</td><td>Classical IP</td></tr><tr><td>9</td><td>ATM MUX</td></tr><tr><td>203</td><td>Ethernet 10BASE-T</td></tr><tr><td>204</td><td>Ethernet 100BASE-T</td></tr><tr><td>205</td><td>Token Ring 4 mbs</td></tr><tr><td>206</td><td>Token Ring 16 mbs</td></tr><tr><td>207</td><td>FDDI</td></tr><tr><td>208</td><td>CDDI</td></tr><tr><td>209</td><td>ATM 25 mbs</td></tr><tr><td>210</td><td>ATM 50 mbs</td></tr><tr><td>211</td><td>DS-1</td></tr><tr><td>212</td><td>DS-3</td></tr><tr><td>213</td><td>OC-3</td></tr><tr><td>214</td><td>OC-12</td></tr><tr><td>215</td><td>OC-48</td></tr></table></div> <div><p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p></div>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

Trap Type	groupChange
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.14
Description	A Group was either created or deleted through the UI or Switch Manager.
Bit Position (Word 1)	13
Hex Value (Word 1)	2000
Trap Text and Variable Descriptions	<div><div>Group created or deleted (vlan 2 admin status 4)</div><div><p>Group number. The Group number that has been created or deleted.</p><p>Administrative status. The administrative status for this group. Possible options are:</p><ol style="list-style-type: none">1 Disabled. All ports in this Group are disabled.2 Enabled. All ports in this Group are enabled.3 Deleted. This Group was deleted, and all attached virtual ports and routers are detached and deleted.4 Created. This Group has been created.5 Modify. This Group has been modified.</div></div>

Trap Type	vlanChange
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.15
Description	A VLAN was either created or deleted through the UI or Switch Manager.
Bit Position (Word 1)	14
Hex Value (Word 1)	4000
Trap Text and Variable Descriptions	<div><div>VLAN Change created or deleted (group 2, admin status 4)</div><div><div>Group number. The Group number to which this VLAN belongs.</div><div>Administrative status. The administrative status for this VLAN. The following integers are valid values:<div><div>1</div><div>Enabled.</div><div>2</div><div>Disabled.</div><div>3</div><div>Deleted. This VLAN was deleted.</div><div>4</div><div>Created. This Group has been created.</div><div>5</div><div>Modify. This Group has been modified.</div></div></div></div></div>

Trap Type	portMove																																												
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.16																																												
Description	The specified port has moved from a Group or has had its configuration changed.																																												
Bit Position (Word 1)	15																																												
Hex Value (Word 1)	8000																																												
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Port VLAN, group or configuration change (slot 2, IF 8, type 4, instance 1) </div> <p>Slot number. The slot number for the module that contains this port.</p> <p>Port number. The port number on this module that was changed.</p> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <table style="margin-left: 40px;"> <tr><td>1</td><td>Unknown</td></tr> <tr><td>2</td><td>Other</td></tr> <tr><td>3</td><td>Router</td></tr> <tr><td>4</td><td>Bridge</td></tr> <tr><td>5</td><td>Trunk</td></tr> <tr><td>6</td><td>ATM trunk port</td></tr> <tr><td>7</td><td>ATM LAN Emulation port</td></tr> <tr><td>8</td><td>Classical IP</td></tr> <tr><td>9</td><td>ATM MUX</td></tr> <tr><td>203</td><td>Ethernet 10BASE-T</td></tr> <tr><td>204</td><td>Ethernet 100BASE-T</td></tr> <tr><td>205</td><td>Token Ring 4 mbs</td></tr> <tr><td>206</td><td>Token Ring 16 mbs</td></tr> <tr><td>207</td><td>FDDI</td></tr> <tr><td>208</td><td>CDDI</td></tr> <tr><td>209</td><td>ATM 25 mbs</td></tr> <tr><td>210</td><td>ATM 50 mbs</td></tr> <tr><td>211</td><td>DS-1</td></tr> <tr><td>212</td><td>DS-3</td></tr> <tr><td>213</td><td>OC-3</td></tr> <tr><td>214</td><td>OC-12</td></tr> <tr><td>215</td><td>OC-48</td></tr> </table> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

Trap	moduleResetReload
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.17
Description	The specified module has been either reset or reloaded. A reload may occur during a firmware download.
Bit Position (Word 1)	16
Hex Value (Word 1)	1 0000
Trap Text and Variable Descriptions	<p>Submodule Type. Indicates the submodule that was reset or reloaded. Typically this value will be 1, meaning the base module was reset or reloaded. If this value is 2, then HSM module 1 was affected. If this value is 3, then HSM module 2 was affected.</p> <p>Slot number. The slot number of the module that was reset or reloaded.</p> <div> Module reset or reloaded by chassis manager (slot 4 subunit 1 type 6 status 3) </div> <p>Module Type. Indicates the module type that was reset or reloaded. The following integers are valid values:</p> <ul style="list-style-type: none"> 4 HSM 5 MPM 6 ESM 8-port 10BASE-T 7 ESM 16-port 8 TSM 6-port UTP/STP 9 FSM FDDI module 10 FSM CDDI module 11 ESM 4-port 12 ASM .5 MB multi-mode 13 ESM 12-port 10BASE-T 14 ESM 6-port universal module 15 MPM version II 16 ATM DS-3 17 FSM FDDI single mode 18 ASM .5 MB single mode 19 ASM UTP 20 ESM 8-port fiber 21 ESM 12-port Telco 22 TSM fiber 23 ASM 2 MB multi-mode 24 ASM 2 MB single mode <p>Operational State. Indicates the current state of the module that was reset or reloaded. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Unknown state. The module may have failed low-level self-test. 2 Invalid. The module may exist, by the chassis does not have control of it. 3 Operational. The module is running fine with no errors. 4 Disabled. The module has been set to disable through the UI or SNMP. 5 Reset. The module has been reset. 6 Loading. The module is in the middle of loading. 7 Testing. The module is in self-test. 8 Warning. A warning was detected during operation. 9 Non-fatal error. A non-fatal error was detected during operation. 10 Fatal error. A fatal error occurred during operation. The module may or may not be functional.

Trap Type	systemEvent
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.18
Description	A potentially fatal error occurred in the system.
Bit Position (Word 1)	17
Hex Value (Word 1)	2 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px; text-align: center;"> Potentially fatal error occurred (trap 10) </div> <p>Event Trap Type. A number that identifies the specific error that occurred in the system. The following integers are valid values:</p> <ul style="list-style-type: none"> 10 Unspecified Log Event 11 Log file full 12 Log file erased 20 Unspecified memory event 21 Memory shortage 30 Unspecified CPU event 31 Long term CPU overload 32 Short term CPU overload 40 Unspecified ffs event 41 Attempt to write to full ffs 42 System/user directed purge 43 Removed imgs/cfgs 44 Exec file removed 45 Config file removed 46 Exec file updated 47 Config file updated 50 Unspecified chassis event 51 Module failed to init 52 Module failed to load 53 Module startup failed 54 Module failed 55 Driver failed

<i>Trap Type</i>	vlanRouteTableFull
<i>Object ID</i>	1.3.6.1.4.1.800.3.1.1.4.0.19
<i>Description</i>	The IP or IPX route table is full.
<i>Bit Position (Word 1)</i>	18
<i>Hex Value (Word 1)</i>	4 0000
<i>Trap Text and Variable Descriptions</i>	IP or IPX route table is full on insertion.

<i>Trap Type</i>	sapTableFull
<i>Object ID</i>	1.3.6.1.4.1.800.3.1.1.4.0.20
<i>Description</i>	The SAP table is full upon insertion.
<i>Bit Position (Word 1)</i>	19
<i>Hex Value (Word 1)</i>	8 0000
<i>Trap Text and Variable Descriptions</i>	SAP table full on insertion.

Trap Type	dlciNew
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.27
Description	Frame Relay DLCI was created.
Bit Position (Word 1)	26
Hex Value (Word 1)	400 0000
Trap Text and Variable Descriptions	<div><div>Frame Relay DLCI created (slot 3 port 1 DLCI Number 100)</div><div><p>Slot number. The slot number where this Frame Relay module is located.</p><p>Port number. The port number on this Frame Relay module where the DLCI was created.</p><p>DLCI number. The number of the DLCI that was just created.</p></div></div>

Trap Type	dlciDel
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.28
Description	Frame Relay DLCI was deleted.
Bit Position (Word 1)	27
Hex Value (Word 1)	800 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 10px; margin: 10px auto; width: fit-content;"> <p>Frame Relay DLCI deleted (slot 3 port 1 DLCI Number 100)</p> </div> <div style="margin-top: 20px;"> <p>Slot number. The slot number where this Frame Relay module is located.</p> <p>Port number. The port number on this Frame Relay module where the DLCI was deleted.</p> <p>DLCI number. The number of the DLCI that was just deleted.</p> </div>

Trap Type	dlciUp
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.29
Description	Frame Relay DLCI changed to active state.
Bit Position (Word 1)	28
Hex Value (Word 1)	1000 0000
Trap Text and Variable Descriptions	<div><div>Frame Relay DLCI Changed to Active (slot 3 port 1 DLCI Number 100)</div><div><p>Slot number. The slot number where this Frame Relay module is located.</p><p>Port number. The port number on this Frame Relay module where the DLCI was activated.</p><p>DLCI number. The number of the DLCI that was just changed to active.</p></div></div>

Trap Type	dlciDn
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.30
Description	Frame Relay DLCI changed to inactive state.
Bit Position (Word 1)	29
Hex Value (Word 1)	2000 0000
Trap Text and Variable Descriptions	<div> <div>Frame Relay DLCI Changed to Inactive (slot 3 port 1 DLCI Number 100)</div> <div> <div>Slot number. The slot number where this Frame Relay module is located.</div> <div>Port number. The port number on this Frame Relay module where the DLCI was de-activated.</div> <div>DLCI number. The number of the DLCI that was just changed to inactive.</div> </div> </div>

Trap Type	portManualForwardingMode																																												
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.31																																												
Description	The specified port was placed into manual mode forwarding as its default setting.																																												
Bit Position (Word 1)	30																																												
Hex Value (Word 1)	4000 0000																																												
Trap Text and Variable Descriptions	<div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;"> <p>Slot number. The slot number where this port is located.</p> </div> <div style="text-align: center;"> <p>Port number. The port number on the module.</p> </div> </div> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin: 10px 0; text-align: center;"> Port placed into manual mode forwarding (slot 3, port 1, type 1, instance 1) </div> <div style="margin-top: 20px;"> <p>Port Type. The physical type of this port. The following integers are valid values:</p> <table style="margin-left: 40px;"> <tbody> <tr><td>1</td><td>Unknown</td></tr> <tr><td>2</td><td>Other</td></tr> <tr><td>3</td><td>Router</td></tr> <tr><td>4</td><td>Bridge</td></tr> <tr><td>5</td><td>Trunk</td></tr> <tr><td>6</td><td>ATM trunk port</td></tr> <tr><td>7</td><td>ATM LAN Emulation port</td></tr> <tr><td>8</td><td>Classical IP</td></tr> <tr><td>9</td><td>ATM MUX</td></tr> <tr><td>203</td><td>Ethernet 10BASE-T</td></tr> <tr><td>204</td><td>Ethernet 100BASE-T</td></tr> <tr><td>205</td><td>Token Ring 4 mbs</td></tr> <tr><td>206</td><td>Token Ring 16 mbs</td></tr> <tr><td>207</td><td>FDDI</td></tr> <tr><td>208</td><td>CDDI</td></tr> <tr><td>209</td><td>ATM 25 mbs</td></tr> <tr><td>210</td><td>ATM 50 mbs</td></tr> <tr><td>211</td><td>DS-1</td></tr> <tr><td>212</td><td>DS-3</td></tr> <tr><td>213</td><td>OC-3</td></tr> <tr><td>214</td><td>OC-12</td></tr> <tr><td>215</td><td>OC-48</td></tr> </tbody> </table> <p>Physical Instance. The specific instance of this slot/port/type. In most cases this value will be 1 (only one instance of the port), but an ATM port may have multiple instances. Possible values range from 1 to 254.</p> </div>	1	Unknown	2	Other	3	Router	4	Bridge	5	Trunk	6	ATM trunk port	7	ATM LAN Emulation port	8	Classical IP	9	ATM MUX	203	Ethernet 10BASE-T	204	Ethernet 100BASE-T	205	Token Ring 4 mbs	206	Token Ring 16 mbs	207	FDDI	208	CDDI	209	ATM 25 mbs	210	ATM 50 mbs	211	DS-1	212	DS-3	213	OC-3	214	OC-12	215	OC-48
1	Unknown																																												
2	Other																																												
3	Router																																												
4	Bridge																																												
5	Trunk																																												
6	ATM trunk port																																												
7	ATM LAN Emulation port																																												
8	Classical IP																																												
9	ATM MUX																																												
203	Ethernet 10BASE-T																																												
204	Ethernet 100BASE-T																																												
205	Token Ring 4 mbs																																												
206	Token Ring 16 mbs																																												
207	FDDI																																												
208	CDDI																																												
209	ATM 25 mbs																																												
210	ATM 50 mbs																																												
211	DS-1																																												
212	DS-3																																												
213	OC-3																																												
214	OC-12																																												
215	OC-48																																												

Trap Type	duplicateIPaddress
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.35
Description	The switch detected a duplicate IP address.
Bit Position (Word 2)	2
Hex Value (Word 2)	4
Trap Text and Variable Descriptions	<div> <div> <p>IP Address. The IP address of the station that reported the duplicate IP address.</p> </div> <div> <p>MAC Address. The Mac address of the station that reported the duplicate IP address.</p> </div> </div> <div> <p>Duplicate IP address detected (IP addr 192.168.10.1, Mac 0036589adf01, slot 3, IF 4, dup Mac 00145221cd02, dup slot 1, dup IF 3)</p> </div> <div> <div> <p>Port number. The port on the module of the reporting station from which the trap was sent.</p> </div> <div> <p>Duplicate slot. The slot number on the reporting station where the duplicate address was discovered.</p> </div> <div> <p>Duplicate port. The port on the module of the reporting station where the duplicate address was discovered.</p> </div> </div> <div> <div> <p>Slot number. The slot number of the reporting station from which the trap was sent.</p> </div> <div> <p>Duplicate MAC. The Mac address associated with the duplicated IP address.</p> </div> </div>

Trap Type	duplicateMACaddress
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.36
Description	The switch detected a duplicate MAC address of one of its own router ports.
Bit Position (Word 2)	3
Hex Value (Word 2)	8
Trap Text and Variable Descriptions	<div><div>Duplicate MAC address detected (Mac 00145221cd02, slot 2, IF 3, time 4)</div><div><div>MAC address. The router port's MAC address for which the last duplicate MAC address was detected.</div><div>Slot. The slot number where the duplicate MAC address was last received.</div><div>Interface. The interface number where the duplicate MAC address was last received.</div><div>Time. The time in seconds when the duplicate MAC was detected.</div></div></div>

<i>Trap Type</i>	healthThresholdRising
<i>Object ID</i>	1.3.6.1.4.1.800.3.1.1.4.0.37
<i>Description</i>	At least one of the user-specified thresholds has exceeded.
<i>Bit Position (Word 2)</i>	4
<i>Hex Value (Word 2)</i>	10
<i>Trap Text and Variable Descriptions</i>	Thresh-hold rising trap

<i>Trap Type</i>	healthThresholdFalling
<i>Object ID</i>	1.3.6.1.4.1.800.3.1.1.4.0.38
<i>Description</i>	At least one of the user-specified thresholds was exceeded during the previous cycle and none of them are exceeded in the current cycle.
<i>Bit Position (Word 2)</i>	5
<i>Hex Value (Word 2)</i>	20
<i>Trap Text and Variable Descriptions</i>	Thresh-hold falling trap

Trap Type	healthThresholdDevice
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.39
Description	At least one of the device-level threshold crossing was detected.
Bit Position (Word 2)	6
Hex Value (Word 2)	40
Trap Text and Variable Descriptions	<div> <p>Device-level threshold crossing is detected (Data 0a 09 0d 53 00 00 00 00 00 00 00 00 00 00 00)</p> <p>Data. An octet string that represents the Contents of device-level rising/falling threshold trap.</p> </div>

Trap Type	healthThresholdModule
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.40
Description	At least one module-level threshold crossing was detected.
Bit Position (Word 2)	7
Hex Value (Word 2)	80
Trap Text and Variable Descriptions	<div> <p>Module-level threshold crossing is detected (count 2, data 0a 09 0d 53 00 00 00 00 00 00 00 00 00 00 00))</p> <p>Count. The number of modules with threshold crossing data in module-level rising/falling threshold traps.</p> <p>Data. An octet string that represents the Contents of device-level rising/falling threshold trap.</p> </div>

Trap Type	xylanXIPXMAPPortStatusChange
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.41
Description	An XMAP turned on or off.
Bit Position (Word 2)	8
Hex Value (Word 2)	100
Trap Text and Variable Descriptions	<div>The status of an XMAP-tracked virtual port has changed (port 1, reason 2)</div> <div>Port number. The virtual port number of the port that most recently changed.</div> <div>Reason. The reason for the last port status change. The following integers are valid values: 0 No trap has been sent. 1 A port was added. 2 A change of information on an existing port. 3 A port was deleted.</div>

Trap Type	xylanXIPXMAPPortStateChange				
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.42				
Description	An XMAP turned on or off.				
Bit Position (Word 2)	9				
Hex Value (Word 2)	200				
Trap Text and Variable Descriptions	<div><p>The state of the XMAP agent has changed to (state 1)</p><p>Operating State. The XMAP's operating state. The following integers are valid values:</p><table><tr><td>1</td><td>inactive</td></tr><tr><td>2</td><td>active</td></tr></table></div>	1	inactive	2	active
1	inactive				
2	active				

Trap Type	clkBusLineStateChange
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.45
Description	Either the bus line's status changed (active or inactive) or clock switching occurred.
Bit Position (Word 2)	10
Hex Value (Word 2)	400
Trap Text and Variable Descriptions	<div><div>Bus Line's status changed (bus line 1, operating state 1) or clock switching has occurred.</div><div><div>Bus line. The specific bus line where the status change occurred. The following integers are valid values: 1 8 khz 2 19 mhz</div><div>Operating State. The bus line's operating state. The following integers are valid values: 1 inactive 2 active</div></div></div>

Trap Type	xylanXIPGMAPFailedUpdate
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.44
Description	GMAP is unable to update the forwarding database to reflect information in its internal database.
Bit Position (Word 2)	11
Hex Value (Word 2)	800
Trap Text and Variable Descriptions	<p>Reason. The reason for the last GMAP update was not applied. The following integers are valid values:</p> <ol style="list-style-type: none"> 1 The target group is an authenticated group. 2 The update would conflict with a binding rule. 3 The update would create two different group entries for the same protocol. 4 The update would create two different protocol entries for the same group. 5) The target group is not mobile. <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin: 10px 0; text-align: center;"> GMAP is unable to update the forwarding database (reason 1, port 2, Mac 0036589adf01, protocol 4, group 5) </div> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 30%;"> <p>MAC address. The last MAC address for which a GMAP change was not applied.</p> </div> <div style="width: 30%;"> <p>Group. The group identifier of the last GMAP change that was not applied.</p> </div> <div style="width: 30%;"> <p>Port. The virtual port number of the last port on which the GMAP change was not applied.</p> </div> </div> <div style="margin-top: 20px;"> <p>Protocol. The protocol identifier of the last GMAP change that was not applied.</p> </div>

Trap Type	avlAuthAttempt
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.43
Description	Indicates the last authenticated VLAN attempt.
Bit Position (Word 2)	16
Hex Value (Word 2)	1 0000
Trap Text and Variable Descriptions	<p>User. The last user who made an authentication attempt.</p> <div> <p>The last VLAN authentication attempt was: (user 1, event 2, MAC 0036589adf01, port 4, slot 5)</p> <p>MAC Address. The last MAC address to make an authentication attempt.</p> <p>Port. The last port number from which the authentication attempt originated.</p> <p>Event type. The last authorization attempt type. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Successful login 2 Failed Login Attempt 3 Logout/Drop <p>Slot. The last slot number from which the authentication attempt originated.</p> </div>

Trap Type	mpcStatisticsOverflow
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.67
Description	A particular entry of the mpcStatisticsTable reached the threshold value.
Bit Position (Word 2)	18
Hex Value (Word 2)	4 0000
Trap Text and Variable Descriptions	<div>GMAP is unable to update the forwarding database (index 1, MPOA replies 3)</div> <div>MPC Index. A unique number which identifies a conceptual row in the mpcConfigTable.</div> <div>MPOA Resolution Replies. The number of MPOA Resolution Replies received with an MPOA CIE Code of 0x81.</div>

Trap Type	mpcShortCut
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.68
Description	The established shortcut path closed or failed to complete the path.
Bit Position (Word 2)	19
Hex Value (Word 2)	8 0000
Trap Text and Variable Descriptions	<p>Row Status. This object allows creation and deletion of MPOA clients.</p> <div> <p>GMAP is unable to update the forwarding database (rowStatus 1, control direct Vci 2, protocol 4, dest addr 192.168.40.12, dest ATM addr 3903488001bc900001020000090020da00000900, index 1, mps index 2)</p> </div> <p>Control Direct VCI. The VCI that identifies the VCC at the point where it connects to a LANE client. If the Control Direct VCC does not exist, this value is zero.</p> <p>Destination ATM Address. The destination ATM address received in the MPOA Resolution Reply.</p> <p>Protocol. The protocol on which flow detection is performed.</p> <p>Destination Address. The destination internet-work layer address.</p> <p>MPC Index. A unique number which identifies a conceptual row in the mpcConifTable.</p> <p>MPC MPS Index. The MPS's index which is used to identify a row in the mpcConig Table.</p>

Trap Type	mpcIngressRetryTimeOut
Object ID	1.3.6.1.4.1.800.3.1.1.4.0.69
Description	The re-try time exceeded the MPC-p5 time.
Bit Position (Word 2)	20
Hex Value (Word 2)	10 0000
Trap Text and Variable Descriptions	<div><p>MPC Index. A unique number which identifies a conceptual row in the mpcConfigTable.</p><p>Maximum Retry Time. The MPC-p5 cumulative maximum value for retry time.</p><p>GMAP is unable to update the forwarding database (index 1, max time 5, dest addr 192.168.40.12, ATM addr 3903488001bc900001020000090020da00000900, protocol 1)</p><p>Destination Address. The destination internet-network layer address.</p><p>Destination ATM Address. The destination ATM address received in the MPOA Resolution Reply.</p><p>Detect Protocol. The protocol on which flow detection is performed.</p></div>

Trap Type	vrrpTrapNewMaster
Object ID	1.3.6.1.2.1.46.1.3.1.0.3
Description	The sending agent has transitioned from “Backup” state to “Master” state.
Bit Position (Word 2)	21
Hex Value (Word 2)	20 0000
Trap Text and Variable Descriptions	<div> <div>Agent has transitioned from Backup to Master state (If index 1, vrid 2)</div> <div> <div>Interface Index Number. A unique value that identifies the sending agent.</div> <div>Virtual Router ID. The number that identifies the virtual router on this VRRP. Possible values range from 1 to 255.</div> </div> </div>

Trap Type	vrrpAuthFailure
Object ID	1.3.6.1.2.1.46.1.3.1.0.4
Description	A packet was received from a router whose authentication key or authentication type conflicts with this router's authentication key or type.
Bit Position (Word 2)	22
Hex Value (Word 2)	40 0000
Trap Text and Variable Descriptions	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> A packet with a wrong authentication key or type is received (If index 1, vrid 2, source 192.168.10.1, error type 3) </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Virtual Router ID. The number that identifies the virtual router on this VRRP. Possible values range from 1 to 255.</p> </div> <div style="width: 45%;"> <p>Packet Source IP. The IP address of an inbound VRRP packet.</p> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 45%;"> <p>Error Type. The type of configuration conflict. The following integers are valid values:</p> <ul style="list-style-type: none"> 1 Invalid authentication type 2 Mismatched authentication 3 Authentication Failure </div> <div style="width: 45%;"> <p>Interface Index Number. A unique value that identifies the sending agent.</p> </div> </div>

Trap Type	bind-violation
Object ID	1.3.6.1.4.1.800.3.1.1.1.0.46
Description	A configured binding rule was violated.
Bit Position (Word 2)	23
Hex Value (Word 2)	80 0000
Trap Text and Variable Descriptions	<p>IP Address. The IP address for which this binding is configured.</p> <p>VLAN ID. The VLAN ID for which this rule has been configured.</p> <p>Group ID. The group ID of the VLAN for which this rule has been configured.</p> <p>A binding rule has been violated (groupId 1, vlanId 2, IP 192.168.10.1 3, Mac 0036589adf01, protocol 5, port 6, rule 4, index 8)</p> <p>Protocol. The protocol for which this binding is configured.</p> <p>Port. The port for which this binding is configured.</p> <p>MAC Address. The MAC address for which this binding is configured.</p> <p>Rule Index. The index which uniquely defines the rule for this vlan.</p> <p>Rule. The rule for which this binding is configured.</p>

Trap Type	pnniRouteConflictPort
Object ID	1.3.6.1.4.1.800.3.1.1.2.0.50
Description	A static route on the pnniIfPortId port was created and this port was configured as a PNNI port. This may cause mis-routing in a PNNI network if the port turns out to be an Inside port.
Bit Position (Word 3)	2
Hex Value (Word 3)	4
Trap Text and Variable Descriptions	<p>Port ID. The port ID number of the port on which the static route is configured.</p> <div> <p>A static route on (port 200) has been created and this port has been configured as a PNNI port (rte addr 3903488001bc90000101, prefix length 80)</p> <p>Route Address. The destination address for which the static route entry is configured.</p> <p>Route Prefix Length. The prefix length of the destination address in the static route entry.</p> </div>

Trap Type	pnniRouteConflictSamePG
Object ID	1.3.6.1.4.1.800.3.1.1.2.0.51
Description	A static route on the pnnixIfPortId port was created and this route matches a prefix of the Peer Group ID.
Bit Position (Word 3)	3
Hex Value (Word 3)	8
Trap Text and Variable Descriptions	<p>Port ID. The port ID number of the port on which the static route is configured.</p> <div> <p>A static route on (port 200) was created and the route matches the Peer Group ID (rte addr 3903488001bc90000101, prefix length 80)</p> </div> <p>Route Address. The destination address for which the static route entry is configured.</p> <p>Route Prefix Length. The prefix length of the destination address in the static route entry.</p>