Broadband Access Aggregation and DSL Configuration Guide, Cisco IOS Release 15.1SG

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

CONTENTS

SNMP traps for PPPoE Session Limits

The SNMP Traps for PPPoE Session Limits feature provides SNMP MIB support for PPPoE session limits and generates notifications if those limits are reached.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SNMP Traps for PPPoE Session Limits

- PPPoE sessions must be established for this feature to work.

Restrictions for SNMP Traps for PPPoE Session Limits

- The **snmp-server enable traps pppoe** command only enables SNMP traps. It does not support inform requests.

Information About SNMP Traps for PPPoE Session Limits

Benefits of Monitoring PPPoE Sessions with SNMP

The monitoring of PPPoE sessions with SNMP provides the following benefits:

- It helps manage the number of PPPoE sessions configured on a router or PVC by sending notification messages when the PPPoE session threshold has been reached.
- It provides a way of tracking PPPoE session information over time.

Network Management Protocol

SNMP is a network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security. SNMP version 2 supports centralized and distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

How to Configure SNMP Traps for PPPoE Session Limits

Configuring the PPPoE Session-Count Threshold for the Router

Perform this task to configure the PPPoE session-count threshold for the router.

Note The **sessions max limit** command is available only if you configure the **bba-group pppoe** command using the **global** keyword.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **bba-group pppoe** {*group-name* | **global**}
5. **sessions max limit** *session-number* [**threshold** *threshold-value*]
6. **virtual-template** *template-number*
7. **end**
8. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE sessions have been reached.

Step 4	**bba-group pppoe** {*group-name* | **global**}
	Example:
	`Router(config)# bba-group pppoe global`
		Configures a BBA group to be used to establish PPPoE sessions and enters BBA group configuration mode.

Step 5	**sessions max limit** *session-number* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions max limit 4000 threshold 3000`	Configures the PPPoE global profile with the maximum number of PPPoE sessions permitted on a router and sets the PPPoE session-count threshold at which an SNMP trap will be generated. **Note** This command applies only to the global profile.

	Command or Action	Purpose
Step 6	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies the virtual template that will be used to clone the virtual access interfaces (VAI).

Step 7	**end**
	Example:
	`Router(config-bba-group)# end`
		Exits BBA group configuration mode and returns to privileged EXEC mode.

Step 8	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for a PVC

Perform this task to configure the PPPoE session-count threshold for a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**]
5. **pvc** [*name*] *vpi* / *vci*
6. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
7. **protocol pppoe**
8. **end**
9. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. - This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.
Step 4	**interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 0/0/0.3 point-to-point`	Configures the ATM interface and enters subinterface configuration mode.
Step 5	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-subif)# pvc 5/120`	Creates an ATM PVC and enters ATM VC configuration mode.
Step 6	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-if-atm-vc)# pppoe max-sessions 5 threshold-sessions 3`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 7	**protocol pppoe** **Example:** `Router(config-if-atm-vc)# protocol pppoe`	Enables PPPoE sessions to be established on ATM PVCs.

Step 8	**end**
	Example:
	`Router(config-if-atm-vc)# end`
		(Optional) Exits ATM VC configuration mode and returns to sub interface mode.

	Command or Action	Purpose
Step 9	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for a VC Class

Perform this task to configure the PPPoE session-count threshold for a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **vc-class atm** *name*
5. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
6. **protocol pppoe** [**group** *group-name* | **global**]
7. **end**
8. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.

	Command or Action	Purpose
Step 4	**vc-class atm** *name* **Example:** `Router(config)# vc-class atm main`	Creates a VC class for an ATM PVC, or SVC, or ATM interface and enters VC class configuration mode.
Step 5	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-vc-class)# pppoe max-sessions 7 threshold-sessions 3`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 6	**protocol pppoe** [**group** *group-name* | **global**] **Example:** `Router(config-vc-class)# protocol pppoe group one`	Enables PPPoE sessions to be established.

Step 7	**end**
	Example:
	`Router(config-vc-class)# end`
		(Optional) Exits VC class configuration mode and returns to privileged EXEC mode.

Step 8	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for an ATM PVC Range

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**]
5. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
6. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
7. **protocol pppoe** [**group** *group-name* | **global**]
8. **end**
9. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. - This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.
Step 4	**interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 0/0/0.3 point-to-point`	Configures the ATM interface and enters the subinterface configuration mode.
Step 5	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-subif)# range pvc 3/100 3/105`	Defines a range of ATM PVCs and enters ATM PVC range configuration mode.
Step 6	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-if-atm-range)# pppoe max-sessions 20 threshold-sessions 15`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.

	Command or Action	Purpose
Step 7	**protocol pppoe** [**group** *group-name* | **global**] **Example:** `Router(config-if-atm-range)# protocol pppoe group two`	Enables PPPoE sessions to be established.

Step 8	**end**
	Example:
	`Router(config-if-atm-range)# end`
		(Optional) Exits ATM PVC range configuration mode and returns to privileged EXEC mode.

Step 9	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for an Individual PVC Within a Range

Perform this task to configure the PPPoE session-count threshold for an individual PVC within an ATM PVC range.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**]
5. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* /end-vci
6. **pvc-in-range** [*pvc-name*] [*vpi* / *vci*]
7. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
8. **end**
9. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. - This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.
Step 4	**interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 6/0.110 multipoint`	Configures the ATM interface and enters subinterface configuration mode.
Step 5	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* /end-vci **Example:** `Router(config-subif)# range range1 pvc 3/100 4/199`	Defines a range of ATM PVCs and enters ATM PVC Range configuration mode.
Step 6	**pvc-in-range** [*pvc-name*] [*vpi* / *vci*] **Example:** `Router(config-if-atm-range)# pvc-in-range pvc1 3/104`	Configures an individual PVC within a PVC range and enters ATM PVC-in-range configuration mode.

	Command or Action	Purpose
Step 7	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(cfg-if-atm-range-pvc)# pppoe max-sessions 10 threshold-sessions 5`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.

Step 8	**end**
	Example:
	`Router(cfg-if-atm-range-pvc)# end`
		(Optional) Exits ATM PVC-in-range configuration mode and returns to privileged EXEC mode.

Step 9	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Monitoring and Maintaining PPPoE Session Counts and SNMP Notifications

Perform the following task to monitor PPPoE sessions counts and SNMP notifications.

SUMMARY STEPS

1. **enable**
2. **debug snmp packets**
3. **debug pppoe errors** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]
4. **debug pppoe** events [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]
5. **show vpdn session**
6. **show pppoe session**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password when prompted.

Example:

```
Router> enable
```

Step 2 **debug snmp packets**

Use this command to display information about every SNMP packet sent or received by the router:

Example:

```
Router# debug snmp packets
SNMP: Packet received via UDP from 192.0.2.11 on GigabitEthernet1/0
SNMP: Get-next request, reqid 23584, errstat 0, erridx 0
 sysUpTime = NULL TYPE/VALUE
 system.1 = NULL TYPE/VALUE
 system.6 = NULL TYPE/VALUE
SNMP: Response, reqid 23584, errstat 0, erridx 0
 sysUpTime.0 = 2217027
 system.1.0 = Cisco Internetwork Operating System Software
 system.6.0 =
SNMP: Packet sent via UDP to 192.0.2.11
```

Step 3 **debug pppoe errors** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

Use this command to display PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.

Example:

```
Router# debug pppoe errors interface atm 1/0.10
PPPoE protocol errors debugging is on
Router#
00:44:30:PPPoE 0:Max session count(1) on mac(00b0.c2e9.c470) reached.
00:44:30:PPPoE 0:Over limit or Resource low. R:00b0.c2e9.c470 L:ffff.ffff.ffff 0/101
ATM1/0.10
```

Step 4 **debug pppoe** events [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

Use this command to display PPPoE protocol messages about events that are part of normal session establishment or shutdown:

Example:

```
Router# debug pppoe events interface atm 1/0.10 vc 101

PPPoE protocol events debugging is on
Router#
00:41:55:PPPoE 0:I PADI  R:00b0.c2e9.c470 L:ffff.ffff.ffff 0/101 ATM1/0.10
00:41:55:PPPoE 0:O PADO, R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM1/0.10
00:41:55:PPPoE 0:I PADR  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM1/0.10
00:41:55:PPPoE :encap string prepared
00:41:55:[3]PPPoE 3:Access IE handle allocated
00:41:55:[3]PPPoE 3:pppoe SSS switch updated
00:41:55:[3]PPPoE 3:AAA unique ID allocated
00:41:55:[3]PPPoE 3:No AAA accounting method list
00:41:55:[3]PPPoE 3:Service request sent to SSS
00:41:55:[3]PPPoE 3:Created  R:0001.c9f0.0c1c L:00b0.c2e9.c470 0/101 ATM1/0.10
00:41:55:[3]PPPoE 3:State REQ_NASPORT    Event MORE_KEYS
00:41:55:[3]PPPoE 3:O PADS  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM1/0.10
00:41:55:[3]PPPoE 3:State START_PPP    Event DYN_BIND
00:41:55:[3]PPPoE 3:data path set to PPP
00:41:57:[3]PPPoE 3:State LCP_NEGO    Event PPP_LOCAL
00:41:57:PPPoE 3/SB:Sent vtemplate request on base Vi2
00:41:57:[3]PPPoE 3:State CREATE_VA    Event VA_RESP
00:41:57:[3]PPPoE 3:Vi2.1 interface obtained
00:41:57:[3]PPPoE 3:State PTA_BIND    Event STAT_BIND
00:41:57:[3]PPPoE 3:data path set to Virtual Access
00:41:57:[3]PPPoE 3:Connected PTA
```

Step 5 **show vpdn session**

Use this command to display information about active Level 2 Forwarding (L2F) protocol tunnel and message identifiers on a VPDN:

Example:

```
Router# show vpdn session
%No active L2TP tunnels
%No active L2F tunnels
PPPoE Session Information Total tunnels 1 sessions 1
PPPoE Session Information
SID        RemMAC          LocMAC        Intf    VASt    OIntf    VC
1       0010.7b01.2cd9  0090.ab13.bca8  Vi4     UP      AT6/0   0/10
```

Step 6 **show pppoe session**

Use this command to display information about the currently active PPPoE sessions:

Example:

```
Router# show pppoe session
     3 sessions in LOCALLY_TERMINATED (PTA) State
     3 sessions total

Uniq ID  PPPoE  RemMAC          Port            VT  VA         State
           SID  LocMAC                              VA-st      Type
      1      1  0007.b3dc.a41c  ATM0/3/1.100     1  Vi2.1      PTA
                001a.3045.0331  VC: 99/100          UP
      2      2  0007.b3dc.a41c  ATM0/3/1.100     1  Vi2.2      PTA
                001a.3045.0331  VC: 99/100          UP
      3      3  0007.b3dc.a41c  ATM0/3/1.100     1  Vi2.3      PTA
                001a.3045.0331  VC: 99/100          UP
Router#
```

Configuration Examples for SNMP Traps for PPPoE Session Limits

Example: Configuring PPPoE Session-Count SNMP Traps

The following example shows how to enable the router to send PPPoE session-count SNMP notifications to the host at the address 192.10.2.10:

```
snmp-server community public RW
```

```
snmp-server enable traps pppoe
snmp-server host 192.10.2.10 version 2c public udp-port 1717
```

Example: Configuring PPPoE Session-Count Threshold for the Router

The following example shows a limit of 4000 PPPoE sessions configured for the router. The PPPoE session-count threshold is set at 3000 sessions, so when the number of PPPoE sessions on the router reaches 3000, an SNMP trap will be generated.

```
bba-group pppoe pppoe1
 sessions max limit 4000 threshold 3000
 virtual-template 1
pppoe limit max-sessions 4000 threshold-sessions 3000
```

Example: Configuring PPPoE Session-Count Threshold for a PVC

The following example shows a limit of five PPPoE sessions configured for the PVC. The PPPoE session-count threshold is set at three sessions, so when the number of PPPoE sessions on the PVC reaches three, an SNMP trap will be generated.

```
interface ATM 0/0/0
 ip address 10.0.0.1 255.255.255.0
 no atm ilmi-keepalive
 pvc 5/120
  protocol ip 10.0.0.2 broadcast
  pppoe max-sessions 5 threshold-sessions 3
  protocol pppoe
```

Example: Configuring PPPoE Session-Count Threshold for a VC Class

The following example shows a limit of seven PPPoE sessions configured for a VC class called "main." The PPPoE session-count threshold is set at three sessions, so when the number of PPPoE sessions for the VC class reaches three, an SNMP trap will be generated.

```
vc-class atm main
  protocol pppoe group global
vc-class atm global
  protocol pppoe
  pppoe max-sessions 7 threshold-sessions 3
```

Example: Configuring PPPoE Session-Count Threshold for a PVC Range

The following example shows a limit of 20 PPPoE sessions configured for the PVC range. The PPPoE session-count threshold will also be 20 sessions because when the session-count threshold has not been explicitly configured, it defaults to the PPPoE session limit. An SNMP trap will be generated when the number of PPPoE sessions for the range reaches 20.

```
interface ATM 0/0/0.3 point-to-point
 range pvc 3/100 3/105
  pppoe max-sessions 20 threshold-sessions 15
  protocol pppoe
```

Example: Configuring PPPoE Session-Count Threshold for an Individual PVC Within a PVC Range

The following example shows a limit of ten PPPoE sessions configured for pvc1. The PPPoE session-count threshold is set at three sessions, so when the number of PPPoE sessions for the PVC reaches three, an SNMP trap will be generated.

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
  pvc-in-range pvc1 3/104
   pppoe max-sessions 10 threshold-sessions 3
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Broadband Access Aggregation and DSL commands	Cisco IOS Broadband Access Aggregation and DSL Command Reference

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for SNMP Traps for PPPoE Session Limits

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for SNMP Traps for PPPoE Session Limits

Feature Name	Releases	Feature Information
SNMP Traps for PPPoe Session Limits	Cisco IOS XE Release 2.6 15.1(1)SG	The SNMP Traps for PPPoE Session Limits feature implements SNMP MIB support for PPPoE session limits and generates notifications in case the limits are reached. The following commands were introduced or modified: **snmp-server enable traps pppoe**.

Extended NAS-Port-Type and NAS-Port Support

The Extended NAS-Port-Type and NAS-Port Support feature allows you to identify what service type is taking place on specific ports with non-RADIUS RFC supported types. You have the flexibility to use your own coding mechanism to track users or to track shared resources, such as Ethernet or ATM interfaces, as you identify traffic based on the service type.

RADIUS attributes are used to define specific authentication, authorization, and accounting (AAA) elements in a user profile. NAS-Port-Type (RADIUS IETF attribute 61) indicates the type of physical port the network access server (NAS) is using to authenticate the user. NAS-Port-ID (RADIUS IEFT attribute 87) contains a text string that identifies the NAS port that is authenticating the user.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Extended NAS-Port-Type and NAS-Port Support

- The device must have RADIUS and AAA enabled.

Information About Extended NAS-Port-Type and NAS-Port Support

Extended NAS-Port-Type (RADIUS Attribute 61)

Prior to the attribute 61 extension, attribute 61 allowed you to identify virtual or Ethernet resources only. Now, by enabling the extended attribute 61 you can also do the following:

- Track specific service port information for broadband environments.
- Identify service port type sessions PPP over ATM (PPPoA), PPP over Ethernet (PPPoE) over Ethernet (PPPoEoE), PPPoE over ATM (PPPoEoA), PPPoE over VLAN (PPPoEoVLAN), and PPPoE over Q-in-Q (PPPoEoQinQ) with a corresponding RADIUS value, which allows you to identify physical NAS port types based on service types.

Benefits of Using the Extended NAS-Port-Type Attribute

The benefits of using the extended attribute 61 are as follows:

- Establishing your own coding scheme to track users on specific physical ports. For example, service providers may want to track customers using shared resources such as Ethernet or ATM interfaces that have virtual LANs (VLANs), stacked VLAN (Q-in-Q), or virtual circuits (VCs) connected to certain customers.
- Allowing additional granularity for subinterfaces such as VLAN, Q-in-Q, VC, or VC ranges by overriding the attribute 61 value to be sent on any session that resides on the port. For example, this capability provides an extra level of detail for service providers in managing their end users and allows for further detail of different customer usage.

The value for the extended 61 attribute can be any number you choose. Customizing your own value is useful when you need to distinguish between NAS port types based on the type of end client using a port. For example, if you want to track mobile clients behind a specific private virtual connection (PVC), you can define your own attribute 61 value for mobile clients.

The non-RFC compliant broadband service port types with their corresponding values that can be set with the extended attribute 61 are shown in the table below.

Table 2 Service Port Types and Corresponding RADIUS Values

Service Port Type	RADIUS Value
Wireless - IEEE 802.16	27

Service Port Type	RADIUS Value
PPPoA	30
PPPoEoA	31
PPPoEoE	32
PPPoEoVLAN	33
PPPoEoQinQ	34

NAS-Port (RADIUS Attribute 5)

NAS-Port (RADIUS attribute 5) indicates the physical NAS port number that is authenticating the user. A logical port can be represented by the virtual path identifier (VPI) and virtual channel identifier (VCI) for an ATM interface, or by the VLAN ID or Q-in-Q ID for an Ethernet interface.

Each platform and service may have different port information, which is relevant to its environment; therefore there is no unique way to populate this attribute. There are four service-specific non configurable formats (**a**, **b**, **c**, and **d**) and one configurable format (**e**) that can be tailored to customer and platform needs.

Format e allowed customization of only one global format for all call types on a device, which had limitations for devices that contained multiple services. With the extended attribute 5 support, it is possible to configure a custom format **e** string for any service type based on the value of attribute 61. When building the RADIUS access or accounting request, the encoding routine will apply the specific format **e** string defined for the session of the value of attribute 61.

Note Setting a specific format **e** string for the value of attribute 61 overrides the default global format **e** string.

Relationship Between NAS-Port-Type (RADIUS Attribute 61) and NAS-Port (RADIUS Attribute 5)

The **radius-server attribute nas-port format**command supports the custom format **e** string with the **type** *nas-port-type* keyword and argument. The **type** keyword allows you to specify format strings to represent physical port types for any of the extended NAS-Port-Type values.

The relationship between extended attribute 61 and extended attribute 5 support is that the format **e** string chosen by the encoding routine will depend on the value of attribute 61 for the session. If you use the extended attribute 61 values (values 30-34) and want to further customize the NAS port type, configure a different format string.

For example, you can specify the string "SSSSAAAAPPPPIIIIIIIICCCCCCCCCCCC" for type 30 (all PPPoA ports), and you can also specify string "SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVV" for type 33 (all PPPoAoVLAN ports). In this case, you can track VPI/VCI-specific information for a PPPoA user and VLAN-specific information for a PPPoEoVLAN user.

Note If you enable the extended attribute 61, format **e** with either type 5 (Virtual) or type 15 (Ethernet) will not function, because these types require an additional value to be set (extended attribute 61 values 30-34).

NAS-Port-ID (RADIUS Attribute 87)

The NAS-Port-ID (RADIUS attribute 87) contains the character text string identifier of the NAS port that is authenticating the user. This text string typically matches the interface description found under the CLI configuration. This attribute is sent by default under IETF attribute 87, it was previously under Cisco vendor-specific-attribute (VSA) Cisco-NAS-Port.

How to Configure Extended NAS-Port-Type and NAS-Port Support

- Configuring Extended NAS-Port-Type Attribute and NAS-Port Attribute Support, page 20
- Overriding Global NAS-Port-Type Configuration, page 22

Configuring Extended NAS-Port-Type Attribute and NAS-Port Attribute Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 61 extended**
4. **radius-server attribute nas-port format** *format* [*string*]
5. **radius-server attribute nas-port format** *format* [*string*] [**type** *nas-port-type*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 61 extended** **Example:** `Device(config)# radius-server attribute 61 extended`	Enables extended non-RFC compliant RADIUS attribute 61 (NAS Port Type, a number) values. These values are sent in an access-request to indicate the type of the NAS physical port, which authenticates the user with a number. • Identifies the following broadband service port types: ◦ IEEE 802.16 ◦ PPPoA ◦ PPPoEoA ◦ PPPoEoE ◦ PPPoEoVLAN ◦ PPPoEoQinQ • Sends the appropriate value to the AAA record. • The value “Virtual” refers to a connection to the NAS through a transport protocol, instead of through a physical port. For example, if a user opens a telnet session with a NAS, the value “Virtual” would be reflected as the NAS value. • There is no specific NAS value for IP sessions. The NAS value depends on the underlying transport technology values described above in Table 1 Service Port Types and Corresponding RADIUS Values, or the value “Virtual” is used for IP sessions.
Step 4	**radius-server attribute nas-port format** *format* [*string*] **Example:** `Device(config)# radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUU`	Configures a global attribute 61 session format string that is used as the default session format. This command does not customize a specific service port type value. • The *format* argument indicates the specific NAS port format. • The *string* argument represents all of a specific port type**.**The characters supported for format, are shown in the **radius-server attribute nas-port format** command page. **Note** If the global format is not set, format **a** is used by default. **Note** You must explicitly define the usage of the 32-bit attribute 5 to use format **e**. The usage is defined with a given parser character for each NAS port field of interest for a given bit field.

	Command or Action	Purpose
Step 5	**radius-server attribute nas-port format** *format* [*string*] [**type** *nas-port-type*] **Example:** `Device(config)# radius-server attribute nas-port format e SSSSAAAAPPPPIIIIIIIICCCCCCCCCCCC type 30`	Configures a specific service port type for extended attribute 61 support. This command does customize a specific service port type value. • The *format* argument indicates the specific NAS port format. • The *string* argument represents all of a specific port type.The characters supported for format **e** are shown in the **radius-server attribute nas-port format** command page. • The **type** keyword allows you to specify different format strings to represent different physical port types. • The *nas-port-type* argument can be set to one of the extended attribute 61 values. **Note** You must explicitly define the usage of the 32-bit attribute 5 to use format **e**. The usage is defined with a given parser character for each NAS port field of interest for a given bit field.

Overriding Global NAS-Port-Type Configuration

You can override attribute 61 configured globally on the router at an interface or subinterface level.

Use the following task to override all global options on how the extended attribute 61 is sent to any subinterface such as Ethernet, VLAN, Q-in-Q, VC, or VC ranges.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number* [*subinterface-number*{**mpls**|**multipoint**|**point-to-point**}]
4. **pvc** [*name*] *vpi* / *vci* [**ces**|**ilmi**|**qsaal**|**smds**|**l2transport**]
5. **radius attribute nas-port-type** *port-number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *interface-number* [*subinterface-number*{**mpls**|**multipoint**|**point-to-point**}] **Example:** `Device(config)# interface atm 5/0/0.1`	Enters ATM subinterface mode.
Step 4	**pvc** [*name*] *vpi* / *vci* [**ces**|**ilmi**|**qsaal**|**smds**|**l2transport**] **Example:** `Device(config-subif)# pvc 1/33`	Enters PVC subinterface mode.
Step 5	**radius attribute nas-port-type** *port-number* **Example:** `Device(config-if-atm-vc)# radius attribute nas-port-type 7`	Sets a specific extended attribute 61 value for an interface or subinterface, select a value for a port type to override the NAS-Port type configured globally. • The range for the *port-number* is 0-2147483647. • The *value* argument must be assigned a number 1-40 to set a customized extended NAS port type and configure a specific service port type. If you choose a number outside of this range, the default global NAS port format **e** string is used to configure the NAS port value that is sent for the session. • You can set a specific service port type with the **radius-server attribute nas-port format** command. This setting overrides a global NAS port type session format.

Step 6	**end**
	Example:
	`Device(config-if-atm-vc)# end`
		Ends the configuration session and returns to privileged EXEC mode.

Configuration Examples for Extended NAS-Port-Type and NAS-Port Support

- Example: Configuring Global Support for Extended NAS-Port-Type Attribute, page 24

- Example: Configuring a Customized Format e String and Port Type, page 24
- Example: Displaying Command Output From a Configured RADIUS Command, page 24

Example: Configuring Global Support for Extended NAS-Port-Type Attribute

The following example shows how to configure global support for extended NAS-Port-Type ports and how to specify two separate format e strings globally for two different types of ports:

- Type 30 (which is PPPoA)
- Type 33 (which is PPPoEoVLAN)

```
Device# configure terminal
Device(config)# radius-server attribute 61 extended
Device(config)# radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUU
Device(config)# radius-server attribute nas-port format e
SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC type 30
Device(config)#
Device(config)# radius-server attribute nas-port format e
SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVV type 33
```

Example: Configuring a Customized Format e String and Port Type

The following example shows how to customize a format **e** string and port type for an ATM interface and then how to override the global value set for extended attribute 61 by applying the customer customized NAS port type value of 36 on the ATM interface:

```
Device# configure terminal
Device(config)# radius-server attribute nas-port format e
SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC type 36
Device(config)# interface atm 5/0/0.1
Device(config-subif)# pvc 1/33
Device(config-if-atm-vc)# radius attribute nas-port-type 36
```

Example: Displaying Command Output From a Configured RADIUS Command

The following example displays command output from a configured RADIUS command, where extended attribute 61 is enabled . You can use the delimiting characters to display only the relevant parts of the configuration.

```
Device# show running-config | include radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
radius-server attribute 61 extended
radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUU
radius-server attribute nas-port format e SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC type 30
radius-server attribute nas-port format e SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC type 31
radius-server attribute nas-port format e SSSSAAAAPPPPVVVVVVVVVVVVVVVVVVVV type 32
radius-server attribute nas-port format e SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVV type 33
radius-server attribute nas-port format e SSSSAPPPQQQQQQQQQQQQVVVVVVVVVVVV type 34
radius-server host 10.76.86.91 auth-port 1645 acct-port 1646
radius-server key rad123
.
.
.
```

The following example displays command output for a configured RADIUS command, where you have globally specified the format **e** string for all PPPoA ports (type 30):

```
Device# show running-config | include radius
```

```
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
radius-server attribute nas-port format e SSSSSSSSAAAAAAAAPPPPPPPPIIIIIIII
radius-server attribute nas-port format e SSSSAAAAPPPPIIIIIIIICCCCCCCCCCCC type 30
radius-server host 10.76.86.91 auth-port 1645 acct-port 1646
radius-server key rad123
.
.
.
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Broadband Access Aggregation and DSL commands	Cisco IOS Broadband Access Aggregation and DSL Command Reference
RADIUS Attributes	*RADIUS Attributes*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Extended NAS-Port-Type and NAS-Port Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3 Feature Information for Extended NAS-Port-Type and NAS-Port Support

Feature Name	Releases	Feature Information
Extended NAS-Port-Type and NAS-Port Support	12.3(7)XI1, 12.2(28)SB, 12.2(33)SRC 15.0(1)M 15.1(1)SG	The Extended NAS-Port-Type and NAS-Port Support feature allows you to identify what service type is taking place on specific ports with non-RADIUS RFC supported types. This feature was introduced to support the Cisco 10000 series router in Cisco IOS Release 12.3(7)XI1. The following commands were introduced or modified: **radius attribute nas-port-type**,**radius-server attribute 61 extended**, **radius-server attribute nas-port format**.