CHAPTER 16

Configuring RADIUS Features

This chapter describes the following features:

RADIUS Attribute Screening

The RADIUS Attribute Screening feature allows you to configure a list of "accept" or "reject" RADIUS attributes on the Cisco 10000 router for authorization and accounting purposes. Based on the accept or reject list you configure for a particular purpose, the Cisco 10000 series router:

- Accepts and processes all standard RADIUS attributes
- Rejects all standard RADIUS attributes

Before you configure a RADIUS accept or reject list, enable AAA using the **aaa new-model** command in global configuration mode. For more information, see the *Cisco IOS Command Summary, Volume 2 of 3, Release 12.2*.

The Cisco 10000 series router supports the RADIUS Attribute Screening feature in the following deployment models:

- Managed L2TP Network Server
- PPP Terminated Aggregation (PTA) to VRF
- Remote Access (RA) to MPLS VPN

Note For more information about RADIUS attribute screening, see the *RADIUS Attribute Screening* feature module.

The RADIUS Attribute Screening feature is described in the following topics:

Feature History for RADIUS Attribute Screening

Cisco IOS Release	Description	Required PRE
12.2(16)BX3	This feature was introduced on the Cisco 10000 series router.	PRE2
12.3(7)XI6	This feature was integrated into Cisco IOS Release 12.3(7) XI6.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Restrictions for RADIUS Attribute Screening

The following restrictions apply to the RADIUS Attribute Screening feature:

- Network Access Server (NAS) Requirement

  To enable the RADIUS Attribute Screening feature, you should configure the Cisco 10000 router, acting as the NAS, for authorization with RADIUS groups.

- Accept or Reject Lists Limitations

  The two filters used to configure accept or reject lists are mutually exclusive; therefore, you can configure only one accept list or one reject list for each purpose and for each server group.

- Vendor-Specific Attributes

  The RADIUS Attribute Screening feature does not support vendor-specific attribute (VSA) screening. However, you can specify attribute 26 (Vendor-Specific) in an accept or reject list, which will accept or reject all VSAs.

- Required Attributes

  Required attributes in a reject list are allowed to pass through. Do not reject the following required attributes:

  - Authorization—6 (Service-Type) and 7 (Framed-Protocol)
  - Accounting—4 (NAS-IP-Address), 40 (Acct-Status-Type), 41 (Acct-Delay-Time), and44 (Acct-Session-ID)

Note When you configure a reject list with required attributes, an error message does not appear because the list does not specify a purpose (authorization or accounting). The server determines if an attribute is required when the attribute's purpose is known.

Prerequisites for RADIUS Attribute Screening

Before you configure a RADIUS accept or reject list, enable AAA using the **aaa new-model** command in global configuration mode. For more information, see the *Cisco IOS Command Summary, Volume 2 of 3, Release 12.2*.

Configuration Tasks for RADIUS Attribute Screening

To configure and verify the RADIUS Attribute Screening feature, see the "Configuring RADIUS Attribute Accept or Reject Lists" section on page 5-37.

Configuration Examples for RADIUS Attribute Screening

This section provides the following configuration examples:

Authorization Accept Configuration Example

The following example shows how to configure an accept list for attribute 6 (Service-Type) and attribute 7(Framed-Protocol). All other attributes (including VSAs) are rejected for RADIUS authorization.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
    attribute 6-7
```

Accounting Reject Configuration Example

The following example shows how to configure a reject list for attribute 66 (Tunnel-Client-Endpoint) and attribute 67 (Tunnel-Server-Endpoint). All other attributes (including VSAs) are accepted for RADIUS accounting.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    accounting reject tnl-x-endpoint
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list tnl-x-endpoint
    attribute 66-67
```

Authorization Reject and Accounting Accept Configuration Example

The following example shows how to configure a reject list for RADIUS authorization and configure an accept list for RADIUS accounting. Although you cannot configure more than one accept or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    authorization reject bad-author
    accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
    attribute 1,40,42-43,46
!
radius-server attribute list bad-author
    attribute 22,27-28,56-59
```

Rejecting Required Attributes Configuration Example

The following example shows debug output for the **debug aaa accounting** command. In this example, required attributes 44, 40, and 41 have been added to the reject list:

```
Router# debug aaa authorization

AAA/ACCT(6): Accounting method=radius-sg (radius)
RADIUS: attribute 44 cannot be rejected
RADIUS: attribute 61 rejected
RADIUS: attribute 31 rejected
RADIUS: attribute 40 cannot be rejected
RADIUS: attribute 41 cannot be rejected
```

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

RADIUS Transmit Retries

The Cisco 10000 router supports an extended RADIUS transmit retries range. Extending the range of RADIUS transmit retries can protect against lost records if the RADIUS server goes down or communication to it is lost.

You use the **radius-server** command to specify the number of times you want the router to retry transmitting to the RADIUS server. The extended range of values is from 1 to a value higher than 17280.

The RADIUS Transmit Retries feature is described in the following topics:

- Feature History for RADIUS Transmit Retries, page 16-43

Feature History for RADIUS Transmit Retries

Cisco IOS Release	Description	Required PRE
12.3(7)XI1	This feature was integrated into Cisco IOS Release 12.3(7) XI1.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Restrictions for RADIUS Transmit Retries

The extended range of RADIUS transmit retries has the following restrictions:

- Using a value at the upper limits of the range of RADIUS transmit retries can force the router to retry for up to 24 hours.
- Using an extended value for RADIUS transmit retries can exhaust the amount of available and allocated buffers.

Configuring RADIUS Transmit Retries

To configure RADIUS transmit retries, enter the following command in global configuration mode:

Command	Purpose
`Router(config)# radius-server host {hostname | ip-address} retransmit retries`	Specifies the number of times the router retransmits to the RADIUS server. The *retries* option is a value from 1 to a number greater than 17280.

Note For more information about available options for the **radius-server** command, see the Cisco IOS Command Reference documentation for Cisco IOS Release 12.2.

Configuration Example for RADIUS Transmit Retries

Example 16-1 configures the router to retransmit up to 5 times to the RADIUS server.

Example 16-1 Configuring RADIUS Transmit Retries

```
Router(config)# radius-server host 10.16.1.2 retransmit 5
```

Monitoring and Troubleshooting RADIUS Transmit Retries

To monitor and troubleshoot RADIUS transmit retries, enter any of the following commands in privileged EXEC mode:

Command	Purpose
`Router# show radius statistics`	Displays the RADIUS statistics for accounting and authentication packets. The Number of RADIUS Timeouts field indicates the number of times a server did not respond and the RADIUS server resent the packet.
`Router# debug radius`	Displays detailed information associated with RADIUS.
`Router# debug radius brief`	Displays abbreviated client/server interaction information and abbreviated minimum packet information.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Extended NAS-Port-Type and NAS-Port Support

In Cisco IOS Release 12.3(7)XI1, support for NAS-Port-Type (RADIUS attribute 61), NAS-Port (RADIUS attribute 5), and NAS-Port-ID (RADIUS attribute 87) were changed in the The Extended NAS-Port-Type Attribute Support feature.

The Extended NAS-Port-Type Attribute Support feature is described in the following topics:

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

Cisco IOS Release	Description	Required PRE
12.3(7)XI1	This feature was introduced on the Cisco 10000 series router.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

NAS-Port-Type (RADIUS Attribute 61)

Remote Authentication Dial-In User Service (RADIUS) attributes are used to define specific Authentication, Authorization, and Accounting (AAA) elements in a user profile, which is stored on the RADIUS daemon. Currently the Internet Engineering Task Force (IETF) RADIUS attributes that are supported include an attribute 61, NAS-Port-Type. NAS-Port-Type indicates the type of physical port the network access server (NAS) is using to authenticate the user.

However there was no method to identify NAS-Port-Type based on a specific broadband service type because the RADIUS RFC does not support extended types that defines these types of ports. Basically all PPPoA, PPPoEoE, and PPPoEoA sessions were identified as being VIRTUAL and all PPPoEoVLAN and PPPoEoQinQ as ETHERNET.

The Extended NAS-Port-Type Attribute Support feature expands NAS-Port-Type, attribute 61, in order that the client can better identify what type of service is taking place on the different types of ports.

One advantage of this feature is that service providers can have their own coding mechanism to track users on given ports differently. Service providers may especially want to track customers using shared resources such as Ethernet or ATM interfaces that have VLANs (or Q-in-Q) and VCs connected to certain customers.

The configuration command **radius-server attribute 61 extended** enables identifying the following new non-RFC compliant, broadband service port types that are indicated by the following numeric values:

- Value 30: PPPoA
- Value 31: PPPoEoA
- Value 32: PPPoEoE
- Value 33: PPPoEoVLAN
- Value 34: PPPoEoQinQ

An additional capability is that subinterfaces such as VLAN, Q-in-Q, VC, or VC ranges are allowed to override the NAS-Port-Type attribute value to be sent on any session that resides on it. This capability provides an extra level of granularity for service providers in managing their end users and allows for further differentiation of different customer usage. This capability is provided with the **radius attribute nas-port-type** [*value*] command.

The value for NAS-Port-Type can be any number chosen by the customer. In particular, customizing your own value is useful when you need to differentiate the NAS-Port-Type based on which type of end client is actually using the port. For example if you want to track mobile clients behind a specific PVC, you can define your own NAS-Port-Type for mobile clients.

NAS-Port (RADIUS Attribute 5)

The NAS-Port (RADIUS attribute 5) is a 32 bit value that uniquely represents the physical or logical port the user is attempting to authenticate on. 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.

Because each platform and service may have different port information which are relevant to their environment, there is no one unique way to populate this attribute. Currently Cisco has 4 hard wired formats (a-d) which are service specific and 1 configurable format (e) which can be tailored to customer and platform-specific needs.

Previously format e only allowed customizing 1 global format for all call types on a device, which limited its usefulness on devices that contained multiple services. With the extended NAS-port support, you can now configure a custom format e string for any and all service types based on the value of the NAS-Port-Type (RADIUS attribute 61). That is, when building the RADIUS Access or Accounting request, the encoding routine will pick the specific format e string defined for the session's NAS-Port-Type value and use that first instead of using the default global format e string.

The only relationship between NAS-Port-Type extensions and NAS-Port extension is that the format e string chosen by the encoding routine will depend on the value of the NAS-Port-Type for the session. Therefore if you use the extended NAS-Port-Type values (values 30-34), you should also configure format e to use them. If you do not use the extended NAS-Port-Type support, then you should use the old values, specifically, value 5 for Virtual and value 15 for Ethernet service port types. Configuring back to these port types can also allow the user to revert to previous behavior for certain interfaces.

The **radius-server attribute nas-port format e** command was enhanced to support the custom format e string with the [**type** *nas-port-type*] keyword and option. The **type** option allows you to specify different format strings to represent different physical types of ports on the Cisco 10000 for any of the extended NAS-Port-Type values. For example, you can specify the string "SSSSAAAAPPPPIIIIIIIICCCCCCCCCCCC" for type 30 (all PPPoA ports), yet you can also specify the string "SSSSAAAAPPPPVVVVVVVVVVVVVVVVVVV" for type 33 (all PPPoAoVLAN ports). In this case, the service provider can track VPI/VCI-specific information for a PPPoA user and VLAN-specific information for a PPPoEoVLAN user.

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 was previously available under Cisco Vendor Specific Attribute (VSA) "cisco-nas-port". But it is now sent by default under the IETF attribute 87 as per customer demand.

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

Authentication, Authorization, and Accounting (AAA) must be enabled and already set up to use RADIUS.

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

To configure Extended NAS-Port-Type and NAS-Port Attributes Support, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# radius-server attribute 61 extended`	Enables extended, non-RFC compliant NAS-Port-Type values, which will identify new broadband service port types, such as PPPoA, PPPoEoA, PPPoEoE, PPPoEoVLAN, and PPPoEoQinQ, and sends the appropriate value to the AAA records.
Step 2	`Router(config)# radius-server attribute nas-port format e` [*string*] [**type** {*nas-port-type*}] Example: `Router(config)# radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUU`	First configure a default NAS-Port format e string that will be used as the default format by a session that has a NAS-Port-Type which is not customized for a specific service port type value. Specify a format string in configurable format e. Format e requires you to explicitly define the usage of the 32 bits of attribute 5 (NAS-Port). The usage is defined with a given parser character for each NAS-Port field of interest for a given bit field. For *string*, the characters supported are: • Zero : 0 • One : 1 • DS0 shelf : f • DS0 slot : s • DS0 adapter : a • DS0 port : p • DS0 subinterface : i • DS0 channel : c • Async shelf : F • Async slot : S • Async port : P • Async Line : L • PPPoX slot : S • PPPoX adapter : A • PPPoX port : P • PPPoX VLAN Id : V • PPPoX VPI : I • PPPoX VCI : C • Session-Id : U • PPPoX Inner VLAN ID: Q For more information on how to define *string*, see the *Cisco IOS Security Command Reference, Release 12.3T.*

	Command	Purpose

Step 3	`Router(config)# radius-server attribute nas-port format e [string] [type {nas-port-type}]`
	
	`Example:`
	`Router(config)# radius-server attribute nas-port format e SSSSAAAAPPPPIIIIIIIICCCCCCCCCCCC type 30`
		Configures a specific service port type for extended NAS-Port-Type support.
		
		The **type** option allows you to specify different format strings to represent different physical types of ports on the Cisco 10000 for any of the extended NAS-Port-Type values. For example, you can specify the string "SSSSAAAAPPPPIIIIIIIICCCCCCCCCCCC" for type 30 (all PPPoA ports), yet you can also specify string "SSSSAAAAPPPPVVVVVVVVVVVVVVVVVVVV" for type 33 (all PPPoAoVLAN ports). In this case, the service provider can track VPI/VCI-specific information for a PPPoA user and VLAN-specific information for a PPPoEoVLAN user.
		
		nas-port-type can be one of the extended NAS-Port-Type values:
		• Value 30: PPPoA
		• Value 31: PPPoEoA
		• Value 32: PPPoEoE
		• Value 33: PPPoEoVLAN
		• Value 34: PPPoEoQinQ

You can override the NAS-Port-Type configured globally on the router at an interface or subinterface level. To override all global options on how the Extended NAS-Port-Type attribute is sent on any interfaces or subinterfaces such as for Ethernet, VLAN, Q-in-Q, VC, or VC ranges, enter the following commands in the PVC submode or Ethernet subinterface mode (beginning in global configuration mode):

	Command	Purpose
Step 1	`Router(config)# interface atm 5/0/0.1`	Enters ATM subinterface mode.
Step 2	`Router(config-subif)# pvc 1/33`	Enters PVC subinterface mode.
Step 3	`Router(config-if-atm-vc)# radius attribute nas-port-type` [*value*]	To set a different extended NAS-Port-Type value for an interface or subinterface, select a value for a port type to override the NAS-Port type configured globally. This feature allows for further differentiation of different customer usage. Select a *value* for NAS-Port-Type. Value can be any number, 0-2147483647, chosen by the customer. In particular, customizing your own value is useful when you need to differentiate the NAS-Port-Type based on which type of end client is actually using the port. For example if you want to track mobile clients behind a specific PVC, you can define your own NAS-Port-Type for mobile clients. **Note** You must choose a number within the range 1-40 for *value* if you wish to set a different customized extended NAS-Port-Type value and do that in conjunction with configuring an extended specific service port type (using the "format e type" command). Choosing a number outside that range will cause the default NAS-port format e string to be used to configure the NAS-Port value that is sent for that session.

Verifying Extended NAS-Port-Type and NAS-Port-ID Attributes Support

To verify the Extended NAS-Port-Type and NAS-Port-ID Attributes Support feature, enter the following command in privileged EXEC mode:

Command	Purpose
`Router# show running-config`	Displays the current configuration of the router. Check the output of this command to confirm the configuration.

The following example displays the current configuration of RADIUS command output, where you have enabled the extended NAS-Port-Types. You can use delimiting characters to display only the relevant parts of the configuration.

```
Router# show run | inc 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 the current configuration of RADIUS command output, where you have globally specified the format e string for all PPPoA ports (type 30).

```
Router# show run | inc 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
```

Configuration Examples for Extended NAS-Port-Type Attribute Support

The following examples show how to configure global support for Extended NAS-Port-Type ports, and to specify two separate e format strings globally but for two different types of ports (type 30 which is PPPoA and type 33 which is PPPoEoVLAN):

```
Router# configure terminal
Router(config)#
Router(config)# radius-server attribute 61 extended

Router(config)# radius-server attribute nas-port format e
SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC type 30
Router(config)#

Router(config)# radius-server attribute nas-port format e
SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVV type 33
Router(config)#
```

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

```
Router# configure terminal
Router(config)# radius-server attribute nas-port format e SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC
type 36

Router(config)# interface atm 5/0/0.1
Router(config-subif)# pvc 1/33
Router(config-if-atm-vc)#
Router(config-if-atm-vc)# radius attribute nas-port-type 36
```

RADIUS Attribute 31: PPPoX Calling Station ID

The RADIUS Attribute 31: PPPoX Calling Station ID feature enables service providers to provide more information about the call originator to the RADIUS server in a DSL environment, such as the physical lines on which customer calls originate. Specifically, this feature allows operators to track customers through the physical lines on which customer calls originate. Service providers can better maintain the profile database of their customers as they move from one physical line to another.

Because this feature provides a virtual port that does not change as customers move from one physical line to another, RADIUS attribute 31 (Calling-Station-ID) can also be used for additional security checks. The Calling-Station-ID attribute is included in both ACCESS-REQUEST and ACCOUNTING-REQUEST messages.

The PPPoX Calling Station ID feature is described in the following topics:

Feature History for PPPoX Calling Station ID

Cisco IOS Release	Description	Required PRE
12.3(7)XI2	This feature was introduced on the Cisco 10000 series router.	PRE2

Calling-Station-ID Formats

The Calling-Station-ID attribute has 2 formats: Nas-Port and MAC-only. For Nas-Port, the system provides to the RADIUS server the host name and domain name of the node, an interface description, and VPI/VCI information (when the session is ATM-based, such as PPPoA or PPPoEoA). The MAC address is provided for PPPoEoE sessions instead of the VPI and VCI information that is provided for ATM-based sessions. For MAC-only, only the MAC address is specified for PPPoEoE sessions.

Table 16-1 summarizes the enabled Calling-Station-ID formats by session type. Notice that if both the MAC-only and Nas-Port types of Calling-Station-ID are enabled, the system provides only the MAC address to the RADIUS server for PPPoEoE sessions.

Table 16-1 Enabled Calling-Station-ID Formats by Session Type

	Enabled Calling-Station ID Format		
Session Type	**MAC-only**	**Nas-Port**	**MAC-only and Nas-Port**
PPPoA	Not applicable	hostname.domainname:int_desc:vpi:vci	hostname.domainname:int_desc:vpi:vci
PPPoEoA	Not applicable	hostname.domainname:int_desc:vpi:vci	hostname.domainname:int_desc:vpi:vci
PPPoEoE	macaddr	hostname.domainname:int_desc:macaddr	macaddr

Table 16-2 describes the Calling-Station-ID attribute fields.

Table 16-2 Calling-Station-ID Attribute Fields

Field	Description
domainname	Configured domain name of the local router
hostname	Configured host name of the local router
int_desc	Description specified for the configured ATM interface
macaddr	MAC address received from the client
vci	Virtual channel identifier (VCI) for the configured ATM interface
vpi	Virtual path identifier (VPI) for the configured ATM interface

Note The RADIUS logical line ID allows operators to download the Calling-Station-ID from RADIUS during the preauthentication phase. The RADIUS Logical Line ID feature allows a download of the attribute at session start time. You should not use the RADIUS Logical Line ID feature with the RADIUS Attribute 31: PPPoX Calling Station ID feature; using both features causes two instances of the attribute in the RADIUS IOS database for a particular user.

Restrictions for PPPoX Calling Station ID

The following restrictions apply to the RADIUS Attribute 31: PPPoX Calling Station ID feature:

- Do not use the RADIUS Logical Line ID feature with the RADIUS Attribute 31: PPPoX Calling Station ID feature. Using both features causes two instances of the attribute in the RADIUS IOS database for a particular user.
- While this feature can be used with any vendor's RADIUS server, some RADIUS servers can require modifications to their dictionary files to allow the Calling-Station-ID attribute to be presented correctly in the RADIUS logs.
- This feature supports only RADIUS; TACACS+ is not supported.
- Currently, PPPoEoVLAN and PPPoEoQinQ do not provide information on VLAN tags; only the MAC address is provided to the RADIUS server.
- RADIUS attribute 31 (Calling-Station-ID) is not supported for L2TP Network Server (LNS) environments. If you enable this attribute on an LNS, the attribute is not sent to the RADIUS server.

Related Documents for PPPoX Calling Station ID

- *RADIUS Logical Line ID* feature guide
- "Configuring Broadband Access: PPP and Routed Bridge Encapsulation" in the *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*
- *Cisco IOS Dial Technologies Configuration Guide, Release 12.2*

Configuration Tasks for PPPoX Calling Station ID

To configure the RADIUS Attribute 31: PPPoX Calling Station ID feature, perform the following configuration tasks:

- Configuring the Calling-Station-ID Format
- Verifying the Calling-Station-ID

Configuring the Calling-Station-ID Format

To configure the Calling-Station-ID format, perform the following task in global configuration mode:

To verify the Extended NAS-Port-Type and NAS-Port-ID Attributes Support feature, enter the following command in privileged EXEC mode:

Command	Purpose
`Router(config)# radius-server attribute 31 pppox format`	*format*—Specifies the type of Calling-Station-ID • **nas-port**—Enables the Nas-Port format of the Calling-Station-ID attribute. • **mac-addr**—Enables the Mac-only format of the Calling-Station-ID attribute. You can enable one or both types of Calling-Station ID. If both the MAC-only and Nas-Port types of Calling-Station-ID are enabled, the system provides only the MAC address to the RADIUS server for PPPoEoE sessions. See Table 16-1 on page 16-52 for a summary of enabled Calling-Station-ID formats by session type.

Verifying the Calling-Station-ID

To verify the Calling-Station-ID, perform the following task in EXEC mode use the **debug radius** command in privileged EXEC mode. The **debug radius** command verifies that RADIUS attribute 31, Calling-Station-ID, is in the ACCESS-REQUEST and ACCOUNTING-REQUEST. Example 16-2 shows sample output of the **debug radius** command.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use

debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Example 16-2 debug radius Command Output

```
*Sep 14 14:54:43.259: RADIUS(00000008): Send Access-Request to 10.0.0.8:1645 id1645/34,
len 121
*Sep 14 14:54:43.259: RADIUS: authenticator C3 81 6B 7A F8 38 F9 FE - E6 82 A6 91 92 54 44
66
*Sep 14 14:54:43.259: RADIUS: Framed-Protocol [7] 6 PPP [1]
*Sep 14 14:54:43.259: RADIUS: User-Name [1] 8 "johndoe"
*Sep 14 14:54:43.259: RADIUS: CHAP-Password [3] 19 *
*Sep 14 14:54:43.259: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
*Sep 14 14:54:43.259: RADIUS: NAS-Port [5] 6 0
*Sep 14 14:54:43.259: RADIUS: NAS-Port-Id [87] 9 "8/0/0/0"
*Sep 14 14:54:43.259: RADIUS: Calling-Station-Id [31] 35
":c10k.xtnet.com:my_interface:00b0.c2ef.8400"
*Sep 14 14:54:43.259: RADIUS: Service-Type [6] 6 Framed [2]
*Sep 14 14:54:43.259: RADIUS: NAS-IP-Address [4] 6 10.0.0.119
```

Configuration Example for PPPoX Calling Station ID

The following PPP termination aggregation (PTA) and L2TP access concentrator (LAC) example shows how to configure your LAC for preauthorization by downloading the Logical Line ID:

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa session-id common
!
hostname c10k
ip domain-name xtnet.com
!-------- hostname and domain name are included in the nas-port type CSID---

vc-class atm ppp_auto1200
  vpn service service_control
  protocol pppoe group PPPOETEST
  encapsulation aal5autoppp Virtual-Template1 group PPPOETEST
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Loopback10
 ip address 172.16.1.1 255.255.255.0
!
interface FastEthernet0/0/0
 ip address 10.0.0.119 255.255.255.0
 speed 100
 full-duplex
!
interface ATM1/0/0
 no ip address
 shutdown
 no atm pxf queuing
 atm ilmi-keepalive
 pvc 0/16 ilmi
!
!
```

```
interface ATM1/0/1
 no ip address
 atm clock INTERNAL
 no atm auto-configuration
 atm ilmi-keepalive
 no atm address-registration
 pvc 0/16 ilmi
!
!
interface ATM1/0/1.111 multipoint
! -----This description is used in the calling-station-id ------
 description test_descr
 pvc 0/100
  class-vc ppp_auto1200
!
 pvc 0/101
  class-vc ppp_auto1200
!
interface GigabitEthernet8/0/0
 ip address 10.10.0.1 255.255.255.0
 negotiation auto
 pppoe enable group PPPOETEST
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool default
 ppp authentication chap callin
!
ip local pool default 3.3.3.1 3.3.3.10
!
radius-server attribute 31 pppox nas-port
radius-server attribute 31 pppox mac-addr
radius-server attribute 32 include-in-access-req
radius-server host 10.0.0.8 auth-port 1645 acct-port 1646 key cisco
```

Related Commands for PPPoX Calling Station ID

Command	Description
ip radius source-interface	Requires RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets

RADIUS Packet of Disconnect

The RADIUS Packet of Disconnect feature consists of a method for terminating a session that has already been connected. This packet of disconnect (POD) is a RADIUS access_request packet and is intended to be used in situations where the authenticating agent server wants to disconnect the user after the session has been accepted by the RADIUS access_accept packet. This may be needed in at least two situations:

- Detection of fraudulent use, which cannot be performed before accepting the session. A price structure so complex that the maximum session duration cannot be estimated before accepting the session. This may be the case when certain types of discounts are applied or when multiple users use the same subscription simultaneously.

- To prevent unauthorized servers from disconnecting users, the authorizing agent that issues the POD packet must include three parameters in its packet of disconnect request. For a session to be disconnected, all parameters must match their expected values at the router. If the parameters do not match, the router discards the packet of disconnect packet and sends a NACK (negative acknowledgement message) to the agent.

The data parameters are the following RADIUS attributes:

- User- Name (RADIUS IETF attribute 1)
- Framed-IP-Address (RADIUS IETF attribute 8)
- Acct-Session-Id (RADIUS IETF attribute 44)
- Session-Svr-Key (vendor-proprietary RADIUS attribute 151)

For information about RADIUS attributes, see Appendix A, "RADIUS Attributes".

The RADIUS Packet of Disconnect feature is discussed in the following topics:

Feature History for RADIUS Packet of Disconnect

Cisco IOS Release	Description	Required PRE
12.3(7)XI1	This feature was introduced on the Cisco 10000 series router.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Benefits for RADIUS Packet of Disconnect

- Ability to terminate an established session

Restrictions for RADIUS Packet of Disconnect

Proper matching identification information must be communicated by the:

- Billing server and router configuration
- Router's original accounting start request
- Server's POD request

Related Documents for RADIUS Packet of Disconnect

- *Cisco IOS Security Configuration Guide, Release 12.2*
- *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*
- *Cisco Access Registrar 3.5 Installation and Configuration Guide*
- RFC 2865, *Remote Authentication Dial-in User Service*

Prerequisites for RADIUS Packet of Disconnect

- Configure AAA as described in *Cisco IOS Security Configuration Guide*, Cisco IOS Release 12.2.

Configuration Tasks for RADIUS Packet of Disconnect

To configure the RADIUS Packet of Disconnect feature, perform the following configuration tasks:

- Configuring AAA POD Server
- Verifying AAA POD Server

Configuring AAA POD Server

To configure the Calling-Station-ID format, perform the following task in global configuration mode:

Command	Purpose
`Router(config)# aaa pod server clients [`*client ip address*`] port` [*port-number*] [**auth-type** {**any**| **all**| **session-key**}] [ignore {session-key | server-key}] **server-key** *string*	Enables inbound user sessions to be disconnected when specific session attributes are presented. *client ip-address*—(Optional) Registers the IP address of all the clients who can send POD requests. If not set, it can receive a POD request from any client. *port-number*—(Optional) The network access server User Datagram Protocol (UDP) port to use for POD requests. Default value is 1700. **auth-type—**(Optional) The type of authorization required for disconnecting sessions. • **any**—Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key). • **all**—Only a session that matches all four key attributes is disconnected. **All** is the default. • **session-key**—Session with a matching session-key attribute is disconnected. All other attributes are ignored. **ignore—**(Optional) Ignore the session key or the server key received in the POD packet for session matching. **server-key—**Configures the shared-secret text string. • *string*—The shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.

Verifying AAA POD Server

To verify that the router is configured correctly to performs an AAA POD server, enter the **show running-configuration** command in privileged EXEC mode to display the command settings for the router.

```
Router# show running-configuration
!
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa pod server clients <ip address> port <port number> auth-type [all/ any/ session-key]
server-key cisco
```

Monitoring and Maintaining AAA POD Server

To monitor an AAA POD server and troubleshoot problems:

- Ensure that the POD port is configured correctly in both the router (using **aaa pod server** command) and the RADIUS server. Both should be the same.
- Ensure that the shared-secret key configured in the router (using **aaa pod server** command) and in the AAA server are the same.
- Use debug commands:
  - **debug aaa pod**—displays debug messages for POD packets
  - **debug aaa authentication**—displays debug messages for authentication
  - **debug aaa accounting**—displays debug messages for accounting records
  - **debug radius**—displays debug messages for RADIUS packets

  The following example shows output from the **debug aaa pod** command and indicates a successful POD request.

```
Router# debug aaa pod
AAA POD packet processing debugging is on
General OS:
AAA POD packet processing debugging is on

Router#
4d18h:  ++++++ POD Attribute List ++++++
4d18h: 6291C598 0 00000009 username(336) 8 pod_user
4d18h: 7085EE1C 0 00000001 nas-ip-address(439) 4 23.3.7.3
4d18h:
4d18h: POD: 2.0.0.210 user pod_user 0.0.0.0 sessid 0x0 key 0x0
4d18h: POD:      Line     User     IDB          Session Id Key
4d18h: POD: Skip          <NULL>   0.0.0.0      0x363      0x0
4d18h: POD: KILL Virtual- pod_user 104.1.2.38   0x421A     0xD4105397
4d18h: POD: Skip Virtual- <NULL>   0.0.0.0      0x421B     0x0
4d18h: POD: Sending ACK from port 3799 to 2.0.0.210/64917
```

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Configuration Example for RADIUS Packet of Disconnect

Example 16-3 provides a configuration example for a router performing as an AAA POD server:

Example 16-3 Configuring a Router as an AAA POD Server

```
Router(config)# aaa pod server server-key xyz123
```