management server password through sessions throttle

management server password

To specify the customer premise equipment (CPE) password that is used in the authentication phase, use the **management server password**command in TR-069 Agent configuration mode.

management server password [{*encryption-typecleartext-password*}] *passwd*

Syntax Description		
encryption-type	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Possible values are as follows: • 0--Specifies that the text immediately following is not encrypted. • 7--Specifies that the text is encrypted using an encryption algorithm defined by Cisco.
cleartext-password	(Optional) Cleartext Cisco WAN Management Protocol (CWMP) password, which is not encrypted.
passwd	The CPE password that is used in the authentication phase. This password will be provided to the auto-configuration server (ACS) when the CPE is challenged for credential as part of authentication during the session establishment.

Command Modes

TR-069 Agent configuration (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

Thefollowing example shows how to specify the CPE password that is used in the authentication phase. In this example, the password is cisco and is not encrypted:

```
Device(config-cwmp)# management server password 0 cisco
```

management server url

To specify the HTTP or HTTPS URL to reach the auto-configuration server (ACS), use the **management server url** command in TR-069 Agent configuration mode.

management server url *acs-url*

Syntax Description

acs-url	The HTTP/HTTPS URL to reach the ACS. This URL is used by the CPE to establish the TR-069 session with the ACS.

Command Modes

TR-069 Agent configuration mode (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows the **management server url** command when specifying an HTTP URL:

```
Device(config-cwmp)# management server url http://172.27.116.78:7547/acs
```

The following example shows the **management server url** command when specifying an HTTPS URL:

```
Device(config-cwmp)# management server url https://172.27.116.78:7547/acs
```

max bandwidth

To specify the total amount of outgoing bandwidth available to switched virtual circuits (SVCs) in the current configuration, use the **max bandwidth**command in interface-ATM-VC configuration mode. To remove the current bandwidth setting, use the **no** form of this command.

max bandwidth *kbps*
no max bandwidth *kbps*

Syntax Description

kbps	Total amount of outgoing bandwidth in kilobits per second available to all SVCs in the current configuration.

Command Default

No default behavior or values

Command Modes

Interface-ATM-VC configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Only the guaranteed cell rate of an SVC is counted toward the maximum bandwidth.

Examples

In following example, an SVC called "svcname" on ATM interface 2/0/0 is configured using the **max bandwidth** command to allow a maximum of 50 Mbps of bandwidth to be used by all of the SVCs in this configuration:

```
interface ATM 2/0/0
 svc svcname
  encapsulation aal5auto
  protocol ppp virtual-template 1
  max bandwidth 50000
```

Related Commands

Command	Description
max vc	Specifies the maximum number of SVCs that can be established using the current configuration.

max vc

To specify the maximum number of switched virtual circuits (SVCs) that can be established using the current configuration, use the **max vc**command in interface-ATM-VC configuration mode. To restore the maximum number of SVCs to the default setting, use the **no** form of this command.

max vc *number*
no max vc *number*

Syntax Description

number	Maximum number of SVCs to be established using the current SVC configuration.

Command Default   4096 SVCs

Command Modes

Interface-ATM-VC configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In following example, an SVC called "svcname" on ATM interface 2/0/0 is configured using the **max vc** command to allow a maximum of 100 SVCs to be established using this configuration:

```
interface ATM 2/0/0
 svc svcname
  encapsulation aal5auto
  protocol ppp virtual-template 1
  max vc 100
```

Related Commands

Command	Description
max bandwidth	Specifies the maximum amount of bandwidth available to all SVCs in the current configuration.
svc	Creates an ATM SVC.

multihop-hostname

To enable a tunnel switch to initiate a tunnel based on the hostname or tunnel ID associated with an ingress tunnel, use the **multihop-hostname** command in VPDN request-dialin subgroup configuration mode. To disable this option, use the **no** form of this command.

multihop-hostname *ingress-tunnel-name*
no multihop-hostname *ingress-tunnel-name*

Syntax Description

ingress-tunnel-name	Network access server (NAS) hostname or ingress tunnel ID.

Command Default

No multihop hostname is configured.

Command Modes

VPDN request-dialin subgroup configuration (config-vpdn-req-in)

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 node route processor (NRP).
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **multihop-hostname** command only on a device configured as a tunnel switch.

The *ingress-tunnel-name* argument must specify either the hostname of the device initiating the tunnel that is to be to be switched, or the tunnel ID of the ingress tunnel that is to be switched.

Removing the request-dialin subgroup configuration removes the **multihop-hostname** configuration.

Examples

The following example configures a Layer 2 Tunneling Protocol (L2TP) virtual private dialup network (VPDN) group on a tunnel switch to forward ingress sessions from the host named LAC-1 through an outgoing tunnel to IP address 10.3.3.3:

```
vpdn-group 11
 request-dialin
 protocol l2tp
 multihop-hostname LAC-1
 initiate-to ip 10.3.3.3
 local name tunnel-switch
```

Related Commands

Command	Description
dnis	Configures a VPDN group to tunnel calls from the specified DNIS, and supports additional domain names for a specific VPDN group.
domain	Requests that PPP calls from a specific domain name be tunneled, and supports additional domain names for a specific VPDN group.

Command	Description
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
vpdn multihop	Enables VPDN multihop.
vpdn search-order	Specifies how the NAS is to perform VPDN tunnel authorization searches.

nas-port-id format c

To specify a format for broadband subscriber access line identification coding that complies with a specific set of defined requirements, use the **nas-port-id format c** command in BBA group configuration mode. To disable this format implementation, use the **no** form of this command.

nas-port-id format c
no nas-port-id format c

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, the default strings for NAS-Port-ID are used.

Command Modes

BBA group configuration (config-bba-group)#

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
Cisco IOS XE 2.3.0	This command was integrated.

Usage Guidelines

The **nas-port-id format c** command defines the following broadband subscriber access line identification (NAS-Port-ID) coding format:

{atm/eth/trunk} NAS_slot/NAS_subslot/NAS_port:XPI:XCI {Circuit-ID/Remote-ID/default string}

- For ATM, XPI is the virtual path identifier (VPI) and XCI is the virtual circuit identifier (VCI).

- For Ethernet, XPI is outer vlan-tag, XCI is inner vlan-tag.

- Requirements for XPI:XCI for Ethernet are as follows:

    - For 802.1Q tunneling (QinQ), the format should be outer vlan-tag:inner vlan-tag. (Prior to Release 12.2(31)SB2, Cisco IOS software supports inner vlan-tag:outer vlan-tag).
    - For single tag VLAN, XPI should be 4096.

- The Circuit-ID tag (if present) must be appended to this string when the **nas-port-id format c** command is used. The format for the Circuit-ID or Remote-ID tag is as follows:

AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port[:ANI_XPI.ANI_XCI]

- The digital subscriber line access multiplexer (DSLAM) should append this information to the broadband remote access server (BRAS), and the BRAS transparently delivers it. If the Circuit-ID or Remote-ID tag is not present in DHCP option 82, a string of 0/0/0/0/0/0 should be appended to the NAS-Port-ID tag.

The following examples illustrate this format:

- NAS-Port-ID = atm 31/31/7:255.65535 guangzhou001/0/31/63/31/127

In this example, the subscriber interface type of the BRAS equipment is an ATM interface, the BRAS slot number is 31, the BRAS subslot number is 31, the BRAS port number is 7, the VPI is 255, and the VCI is 65535. The string guangzhou001/0/31/63/31/127 is the Circuit-ID or Remote-ID tag.

- NAS-Port-ID = eth 31/31/7:1234.2345 0/0/0/0/0/0

In this example, the subscriber interface type of the BRAS equipment is an Ethernet interface, the BRAS slot number is 31, the BRAS subslot number is 31, the BRAS port number is 7, the outer vlan-tag is 1234, and the inner vlan-tag is 2345. The string 0/0/0/0/0/0 is the default.

- NAS-Port-ID = eth 31/31/7:4096.2345 0/0/0/0/0/0

In this example, the subscriber interface type of the BRAS equipment is an Ethernet interface, the BRAS slot number is 31, the BRAS subslot number is 31, the BRAS port number is 7, and the VLAN ID is 2345. The string 0/0/0/0/0/0 is the default.

Examples

The following example lists the commands for entering BBA group configuration mode and identifying a profile, configuring a virtual template, and specifying format c for the NAS-Port-ID tag:

```
Router(config)# bba-group pppoe bba-pppoeoe
Router(config-bba-group)# virtual-template 1
Router(config-bba-group)# nas-port-id format c
!
```

Related Commands

Command	Description
bba-group pppoe	Enters BBA group configuration mode and defines a PPPoE profile.
virtual-template	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces.

nas-port format d (bba)

To set the PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format d service, use the **nas-port format d** command in BBA group configuration mode. To remove the extended NAS-Port format, use the **no** form of this command.

nas-port format d *slot* / *adapter* / *port* [**transmit**]
no nas-port format d *slot* / *adapter* / *port*

Syntax Description

slot / *adapter* / *port*	*slot* --Number of bits to store slot number. The range is from 0 to 8.
	adapter --Number of bits to accommodate the adapter value. The range is from 0 to 8.
	port --Number of bits to accommodate the port value. The range is from 0 to 8.
transmit	(Optional) Sends the format to the RADIUS or L2TP Network Server (LNS).

Command Default

If this command is not applied under bba-group mode, the default behavior is to use AAA configured format format d, where *slot* is 4 bits, *adapter* is 1 bit, and *port* is 3 bits.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **nas-port format d** command is applicable only for PPPOE over Ethernet (PPPoEoE) and PPPoE over ATM (PPPoEoA). It does not apply to PPP over ATM (PPPoA). This command can be used if the slot, adapter, and port values are in a different format and need to be changed to the d 4/1/3 format.

Examples

The following example show how to set the PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format d:

```
Router# configure terminal
Router(config)# bba-group pppoe global
Router(config-bba-group)# nas-port format d 2/2/4
```

Related Commands

Command	Description
nas-port-id format c	Specifies a format for broadband subscriber access line identification coding that complies with a specific set of defined requirements.

operating mode

To select an asymmetric digital subscriber line (ADSL) or very high speed digital subscriber line (VDSL) mode of operation, use the operating mode command in controller configuration mode. To restore the default, use the **no** form of this command.

For the 887VA and 887VA-M
operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | ansi}
no operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | ansi}

For the 886VA
operating mode {auto [tone low] | adsl1 [tone low] | adsl2 [tone low] | adsl2+ [tone low] | vdsl2}
no operating mode [{auto [tone low] | adsl1 [tone low] | adsl2 [tone low] | adsl2+ [tone low] | vdsl2}]

Syntax Description

auto	Trains-up to the mode configured on the digital subscriber line access multiplexer.
adsl1	Configures the router to ADSL1 mode.
adsl2	Configures the router to ADSL2 mode.
adsl2+	Configures the router to ADSL2+ mode.
vdsl2	Configures the router to VDSL2 mode.
ansi	Configures the router to ANSI[1] mode.
tone low	Sets the carrier tone range from 29 to 48, C886VA only.

[1] ANSI = American National Standards Institute

Command Default auto

Command Modes

Controller configuration

Command History

Release	Modification
15.1(2)T	This command was introduced on the Cisco 886VA.

Usage Guidelines This command enables customer premise equipment to be manually or automatically configured. It can be manually configured in either ADSL1/2/2+, VDSL2, or ANSI modes. Using the auto mode, the CPE automatically trains-up to the mode configured on the digital subscriber line access multiplexer (DSLAM).

Examples

Note It is recommended to use operating mode auto (default). Using a configuration other than the default configuration for the operating mode can lead to unpredictable behavior on the DSL line.

The following example shows a typical customer premise equipment (CPE) configuration set to auto mode. Outputs in bold are critical. When configured in auto (default), the operating mode command line interface (CLI) is not displayed in the show running command as illustrated in this example.

```
Router# show running
Building configuration...
Current configuration : 1250 bytes
!
! Last configuration change at 02:07:09 UTC Tue Mar 16 2010
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 10
ip source-route
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO887-V2-K9 sn FHK1313227E
license boot module c880-data level advipservices
!
!
vtp domain cisco
vtp mode transparent
!
!
controller VDSL 0
!
vlan 2-4
!
!
!
!
!
interface Ethernet0
 no ip address
no fair-queue
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
 isdn termination multidrop
!
interface ATM0
 no ip address
```

```
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 ip address 30.0.0.1 255.255.255.0
 pvc 15/32
  protocol ip 30.0.0.2 broadcast
!
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
```

end

parameter change notify interval

To set the time interval for the parameter change notifications, use the **parameter change notify interval**command in TR-069 Agent configuration mode.

parameter change notify interval *time-interval*

Syntax Description

time-interval	The time interval, in seconds, for the parameter change notifications. The range for the time interval is 15 to 300. The default value is 60.

Command Default

The time interval is 60 seconds.

Command Modes

TR-069 Agent configuration mode (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following shows how to set the time interval for the parameter change notifications to 75 seconds:

```
Device(config-cwmp)# parameter change notify interval 75
```

pppoe-client control-packets vlan cos

To enable class of service (CoS) marking for PPP over Ethernet (PPPoE) control packets on the PPPoE client, use the **pppoe-client control-packets vlan cos** command in either interface configuration mode or ATM virtual circuit configuration mode. To disable CoS marking for PPPoE control packets on the PPPoE client, use the **no** form of this command.

pppoe-client control-packets vlan cos *number*
no pppoe-client control-packets vlan cos *number*

Syntax Description

number	CoS marking value for PPPoE control packets. The range is from 0 to 7. The default is 0.

Command Default

The CoS value is set to 0.

Command Modes

Interface configuration (config-if)

ATM virtual circuit configuration (config-if-atm-vc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Marking a packet with a CoS value allows you to associate a Layer 2 CoS value with a packet. You can set up to eight different CoS markings.

Examples

The following example shows how to set the CoS marking for PPPoE control packets on the PPPoE client:

```
Router# configure terminal
Router(config)# interface atm0/1/0.1 point-to-point
Router(config-if)# pvc 9/117
Router(config-if-atm-vc)# pppoe-client control-packets vlan cos 2
```

pppoe-client dial-pool-number

To configure a PPP over Ethernet (PPPoE) client and to specify the dial-on-demand routing (DDR) functionality, use the **pppoe-client dial-pool-number** command in interface configuration mode or ATM virtual circuit configuration mode. To disable the configured dial-on-demand functionality, use the **no** form of this command.

pppoe-client dial-pool-number *number* [{**dial-on-demand** | **restart** *number* | **service-name** *name* | **mac-override**}]

no pppoe-client dial-pool-number *number* [{**dial-on-demand** | **restart** *number* | **service-name** *name* | **mac-override**}]

Syntax Description

number	A number that is assigned to a configured dialer pool. The range is from 1 to 255.
dial-on-demand	(Optional) Enables the DDR functionality for the PPPoE connection.
restart *number*	(Optional) Allows the timer to be configured in seconds. The range is from 1 to 3600. The default value is 20.
service-name *name*	(Optional) Specifies the service name requested by the PPPoE client. • The service name that allows the PPPoE client to signal a service name to the Broadband Access Aggregation System (BRAS). • By default, no service name is signaled and the service name value is set to NULL.
mac-override	(Optional) Specifies the MAC address to be used as the local MAC address in the corresponding dialer interface when a session is established.

Command Default

A PPPoE client is not configured and the DDR functionality is disabled.

Command Modes

Interface configuration (config-if)

ATM virtual circuit configuration (config-if-atm-vc)

Command History

Release	Modification
12.1(3)XG	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(13)T	This command was modified. The **dial-on-demand** keyword was added to allow the configuration of the DDR interesting traffic control list functionality.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T and the PPPoE client functionality was modified to support multiple clients on a single ATM PVC.
15.2(4)M	This command was modified. The **mac-override** keyword was added.

Usage Guidelines

One PVC supports multiple PPPoE clients, enabling second line connection and redundancy. Use the **pppoe-client dial-pool-number** command to configure one or more concurrent client PPPoE sessions on a single ATM PVC. When a PPPoE session is established in a single PVC, a MAC address that is configured on a dialer interface is used as the local address for multiple PPPoE clients.

Use this command to configure the DDR interesting traffic control list functionality of the dialer interface with a PPPoE client. When the DDR functionality is configured for this command, the following DDR commands must also be configured: **dialer-group**, **dialer hold-queue**, **dialer idle-timeout**, and **dialer-list**.

Tips for Configuring the Dialer Interface

If you are configuring a hard-coded IP address under the dialer interface, you can configure a default IP route using the **ip route** command:

```
ip route 0.0.0.0 0.0.0.0 dialer1
```

But, if you are configuring a negotiated IP address using the **ip address negotiated** command under the dialer interface, you must configure a default IP route using the **ip route** command:

```
ip route 0.0.0.0 0.0.0.0 dialer1 permanent
```

The reason for this configuration is that the dialer interface will lose its IP address when a PPPoE session is brought down (even if the dialer does not go down), and thereby risk removing routes and all IP routes pointed at the dialer interface, including the default IP route. Although the default IP routed back within a minute by IP background processes, you may risk losing incoming packets during the interval.

Examples

The following example shows how to configure multiple PPPoE clients on a single ATM PVC:

```
Device(config)# interface ATM0
Device(config-if)# no ip address
Device(config-if)# no ip mroute-cache
Device(config-if)# no atm ilmi-keepalive
Device(config-if)# pvc 4/20
Device(config-if)# pppoe-client dial-pool-number 1
Device(config-if)# pppoe-client dial-pool-number 2
```

The following example shows how to configure restart time:

```
Device(config)# pppoe-client dial-pool-number 8 restart 80 service-name "test 4"
Device(config)# pppoe-client dial-pool-number 2 dial-on-demand restart 10
```

The following example shows how to configure multiple PPPoE clients on a dialer PVC interface with a configurable MAC address:

```
Device(config)# interface ATM0
Device(config-if)# no ip address
Device(config-if)# no atm ilmi-keepalive
Device(config-if)# pvc 1/32
Device(config-if)# pppoe-client dial-pool-number 2 mac-override
Device(config-if)# pppoe-client dial-pool-number 1 mac-override

Device(config)# interface Dialer1
Device(config-if)# mac-address aaaa.aaaa.aaaa
Device(config-if)# ip address negotiated
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 1

Device(config)# interface Dialer2
Device(config-if)# mac-address 0002.0002.0002
Device(config-if)# ip address negotiated
```

```
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 2
```

PPPoE Client DDR Idle Timer on an Ethernet Interface

The following example shows how to configure the PPPoE client DDR idle timer on an Ethernet interface and includes the required DDR commands:

```
Device(config)# vpdn enable
Device(config)# no vpdn logging

Device(config)# vpdn-group 1
Device(config)# request-dialin
Device(config)# protocol pppoe

Device(config)# interface Ethernet1
Device(config-if)# pppoe enable
Device(config-if)# pppoe-client dial-pool-number 1 dial-on-demand

Device(config)# interface Dialer1
Device(config-if)# ip address negotiated
Device(config-if)# ip mtu 1492
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 1
Device(config-if)# dialer idle-timeout 180 either
Device(config-if)# dialer hold-queue 100
Device(config-if)# dialer-group 1
Device(config-if)# dialer-list 1 protocol ip permit
```

PPPoE Client DDR Idle Timer on an ATM PVC

The following example shows how to configure the PPPoE client DDR idle timer on an ATM PVC interface and how to include the required DDR commands:

```
Device(config)# vpdn enable
Device(config)# no vpdn logging

Device(config)# vpdn-group 1
Device(config)# request-dialin
Device(config)# protocol pppoe

Device(config)# interface ATM2/0
Device(config-if)# pvc 2/100
Device(config-if)# pppoe-client dial-pool-number 1 dial-on-demand

Device(config)# interface Dialer1
Device(config-if)# ip address negotiated
Device(config-if)# ip mtu 1492
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 1
Device(config-if)# dialer idle-timeout 180 either
Device(config-if)# dialer hold-queue 100
Device(config-if)# dialer-group 1
Device(config-if)# dialer-list 1 protocol ip permit
```

Related Commands	Command	Description
	debug ppp negotiation	Displays LCP and NCP session negotiations.
	debug vpdn pppoe-data	Displays PPPoE session data packets.
	debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be terminated.
	debug vpdn pppoe-events	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
	debug vpdn pppoe-packets	Displays each PPPoE protocol packet exchanged.
	dialer-group	Controls access by configuring a virtual access interface to belong to a specific dialing group.
	dialer hold-queue	Allows interesting outgoing packets to be queued until a modem connection is established.
	dialer idle-timeout	Specifies the idle time before the line is disconnected.
	dialer-list	Defines a DDR dialer list to control dialing by a protocol or by a combination of a protocol and an access list.
	ip address negotiated	Specifies the IP address for a particular interface that is obtained via PPP/IPCP address negotiation.
	ip route	Allows static routes to be established.
	show pppoe session	Displays information about currently active PPPoE sessions.

ppp ip address-save aaa-acct-vsa

To enable IPv4 address conservation, use the **ppp ip address-save aaa-acct-vsa** command in global configuration mode. To disable IPv4 address conservation, use the **no** form of this command.

ppp ip address-save aaa-acct-vsa *vsa-string* **password** {*encryption-type address-save-password address-save-password*}
no ppp ip address-save

Syntax Description

vsa-string	Vendor-specific attribute (VSA). The range is 0 to 32 alpha-numeric characters.
password	Specifies the outbound address-save password.
encryption-type	Type of encryption used, if any. • **0**—Specifies that the subsequent text is not encrypted. • **7**—Specifies that the text is encrypted using an encryption algorithm defined by Cisco.
address-save-password	User-configurable Internet Protocol Control Protocol (IPCP) authorization password. The range is 0 to 32 alphanumeric characters.

Command Default IPv4 address conservation is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
Cisco IOS XE Release 3.8S	This command was modified. The **password** keyword was added.

Usage Guidelines Use this command to enable conservation of IPv4 addresses when a service provider in a dual-stack environment has a limited pool of IPv4 addresses for subscriber allocation. The *vsa-string* argument value is sent to the RADIUS server, which conserves IPv4 address space by assigning an IPv4 address to a customer premises equipment (CPE) only when needed and releasing it after a defined time interval.

Examples The following example shows how to configure IPv4 address conservation:

```
Device(config)# ppp ip address-save aaa-acct-vsa cisco password 0 Cisco123
```

ppp ipcp

To configure PPP IP Control Protocol (IPCP) features such as the ability to provide primary and secondary Domain Name Server (DNS) and Windows Internet Naming Service (WINS) server addresses, and the ability to accept any address requested by a peer, use the **ppp ipcp** command in template or interface configuration mode. To disable a PPP IPCP feature, use the no form of this command.

ppp ipcp {**accept-address** | **address** {**accept** | **required** | **unique**} | **dns** {*primary-ip-address* [*secondary-ip-address*] [**aaa**] [**accept**] | **accept** | **reject** | **request** [**accept**]} | **header-compression ack** | **ignore-map** | **mask** {*subnet-mask* | **reject** | **request**} | **username unique** | **wins** {*primary-ip-address* [*secondary-ip-address*] [**aaa**] [**accept**] | **accept** | **reject** | **request** [**accept**]}}
no ppp ipcp {**accept-address** | **address** {**accept** | **required** | **unique**} | **dns** | **header-compression ack** | **ignore-map** | **mask** | **predictive** | **username unique** | **wins**}

Syntax Description

accept-address	Accepts any nonzero IP address from the peer.
address	Specifies IPCP IP address options: • **accept** --Accepts any nonzero IPv4 or IPv6 address from the peer. • **required** --Disconnects the peer if no IP address is negotiated. • **unique** --Disconnects the peer if the IP address is already in use.

dns	Specifies DNS options:
	
	• *primary-ip-address* --IP address of the primary DNS server.
	
	    • *secondary-ip-address*--(Optional) IP address of the secondary DNS server.
	    • **aaa**--(Optional) Uses DNS data from the AAA server.
	    • **accept**--(Optional) Specifies that any nonzero DNS address will be accepted.
	
	• **accept** --Specifies that any nonzero DNS address will be accepted.
	
	• **reject** --Rejects the IPCP option if received from the peer.
	
	• request--Requests the DNS address from the peer.

header-compression ack	Enables IPCP header compression.
ignore-map	Ignores the dialer map when negotiating the peer IP address.
mask	Specifies IP address mask options: • *subnet-mask* --Specifies the subnet mask to offer the peer. • **reject** --Rejects subnet mask negotiations. • **request** --Requests the subnet mask from the peer.
username unique	Ignores a common username when providing an IP address to the peer.

wins	Specifies WINS options:
	• *primary-ip-address* --IP address of the primary WINS server.
	• *secondary-ip-address*--(Optional) IP address of the secondary WINS server.
	• .**aaa**--(Optional) Use WINS data from the AAA server.
	• **accept**--(Optional) Specifies that any nonzero WINS address will be accepted.
	• **accept** --Specifies that any nonzero WINS address will be accepted.
	• **reject** --Reject the IPCP option if received from the peer.
	• request--Request the WINS address from the peer.

Command Default No servers are configured, and no address request is made.

Command Modes

Template configuration
Interface configuration (config-if)

Command History

Release	Modification
12.0(6)T	This command was introduced.
12.1(5)T	This command was modified. The **reject** and **accept**keywords were added.
Cisco IOS XE Release 3.2S	This command was modified. Support for IPv6 was added.

Examples

The following examples show use of the **ppp ipcp** command:

```
ppp ipcp accept-address
ppp ipcp dns 10.1.1.3
ppp ipcp dns 10.1.1.3 10.1.1.4
ppp ipcp dns 10.1.1.1 10.1.1.2 accept
ppp ipcp dns accept
ppp ipcp dns reject
ppp ipcp ignore-map
ppp ipcp username unique
ppp ipcp wins 10.1.1.1 10.1.1.2
ppp ipcp wins accept
```

The following examples show how to use the **no** form of the **ppp ipcp** command:

```
no ppp ipcp wins
no ppp ipcp ignore-map
```

Related Commands

Command	Description
debug ppp	Displays information on traffic and exchanges in an internetwork implementing the PPP.

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip interfaces	Displays the usability status of interfaces configured for IP.

ppp ipv6cp address unique

To verify if the IPv6 prefix delegation is unique using a PP-enabled interface, and to disconnect the session if the peer IPv6 prefix is duplicated, use the **ppp ipv6cp address unique**command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ppp ipv6cp address unique
no ppp ipv6cp address unique

Syntax Description

This command has no arguments or keywords.

Command Default

Verification of the uniqueness of the IPv6 prefix delegation is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following example shows how to verify whether the IPv6 prefix delegation is unique using a PPP-enabled interface, and to disconnect the session if the peer IPv6 prefix is duplicated:

```
Router> enable

Router# configure terminal
Router(config)# interface virtual-template 5
Router(config-if)# ppp ipv6cp address unique
```

ppp lcp echo mru verify

To verify the negotiated maximum receive unit (MRU) and adjust the PPP virtual access interface maximum transmission unit (MTU), use the **ppp lcp echo mru verify** command in BBA group configuration mode. To disable the effect of the minimum value, use the **no** form of this command.

ppp lcp echo mru verify [**minimum** *value*]
no ppp lcp echo mru verify [**minimum** *value*]

Syntax Description

minimum	(Optional) Indicates that the value specified is a minimum. If a minimum value is specified, the echo request of that size is sent out on the Link Control Protocol (LCP) connection.
value	(Optional) The minimum echo size sent out on the (LCP) connection. The value can be any integer from 64 to 1500.

Command Default

Timeout on verification requests is the same as the PPP LCP finite state machine (FSM) value.

Command Modes

BBA group configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

This command is entered under the virtual-template interface as a troubleshooting aid to verify the value for the negotiated MRU and to adjust the PPP virtual access interface MTU. The timeout on those verification echo requests would be the same as the PPP LCP FSM timeout. The failure of two such echo requests would be construed as the network not supporting that specific MTU. If a minimum value is configured, echo requests of that alternate size are sent out on the LCP connection. If the minimum value is not configured, or if minimum echo requests also fail, then the PPP session is brought down.

If the verification of minimum MTU succeeds, the PPP connection's interface MTU is set to that value. This reset is useful when you troubleshoot and need to adjust the sessions according to underlying physical network capability. After this command is configured, IP Control Protocol (IPCP) is delayed until verification of the MTU is completed at the LCP.

Examples

The following example shows the configuration of two PPPoE profiles:

```
virtual-template 1
 ppp lcp echo mru verify minimum 1200
!
virtual-template 2
 ppp lcp echo mru verify minimum 1200
```

Related Commands

Command	Description
bba-group pppoe	Enters BBA group configuration mode and defines a PPPoE profile.

Command	Description
virtual template	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces.

ppp multilink

To enable Multilink PPP (MLP) on an interface and, optionally, to enable Bandwidth Allocation Control Protocol (BACP) and its Bandwidth Allocation Protocol (BAP) subset for dynamic bandwidth allocation, use the **ppp multilink** command in interface configuration mode. To disable Multilink PPP or, optionally, to disable only dynamic bandwidth allocation, use the **no** form of this command.

ppp multilink [**bap**]
no ppp multilink [**bap** [**required**]]

Cisco 10000 Series Router
ppp multilink
no ppp multilink

Syntax Description

bap	(Optional) Specifies bandwidth allocation control negotiation and dynamic allocation of bandwidth on a link.
required	(Optional) Enforces mandatory negotiation of BACP for the multilink bundle. The multilink bundle is disconnected if BACP is not negotiated.

Command Default This command is disabled. When BACP is enabled, the defaults are to accept calls and to set the timeout pending at 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)SX	This command was implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR-PRE2.
12.2(31)SB 2	This command was integrated into Cisco IOS Release 12.2(31)SB 2.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines This command applies only to interfaces that use PPP encapsulation.

MLP and PPP reliable links do not work together.

When the **ppp multilink**command is used, the first channel will negotiate the appropriate Network Control Protocol (NCP) layers (such as the IP Control Protocol and IPX Control Protocol), but subsequent links will negotiate only the link control protocol and MLP. NCP layers do not get negotiated on these links, and it is normal to see these layers in a closed state.

This command with the **bap** keyword must be used before configuring any **ppp bap** commands and options. If the **bap required** option is configured and a reject of the options is received, the multilink bundle is torn down.

The **no** form of this command without the **bap** keyword disables both MLP and BACP on the interface.

The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

Before Cisco IOS Release 11.1, the **dialer-load threshold 1** command kept a multilink bundle of any number of links connected indefinitely, and the **dialer-load threshold 2** command kept a multilink bundle of two links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a very high idle timer.

Note   By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the MLP bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Cisco 10000 Series Router

The ppp multilink command has no arguments or keywords.

Examples   The following partial example shows how to configure a dialer for MLP:

```
interface Dialer0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 10.0.0.1 name atlanta broadcast 81012345678901
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

Related Commands

Command	Description
compress	Configures compression for LAPB, PPP, and HDLC encapsulations.
dialer fast-idle (interface)	Specifies the idle time before the line is disconnected.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication is selected on the interface.

Command	Description
ppp bap timeout	Specifies nondefault timeout values for PPP BAP pending actions and responses.
ppp chap hostname	Enables a router calling a collection of routers that do not support this command to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on a MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink mrru	Configures the MRRU value negotiated on an MLP bundle.
ppp multilink slippage	Defines the constraints that set the MLP reorder buffer size.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp multilink fragment disable

To disable packet fragmentation, use the **ppp multilink fragment disable** command in interface configuration mode. To enable fragmentation, use the **no** form of this command.

ppp multilink fragment disable
no ppp multilink fragment disable

Syntax Description   This command has no arguments or keywords.

Command Default   Fragmentation is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **ppp multilink fragmentation**.
12.2	The **no ppp multilink fragmentation** command was changed to **ppp multilink fragment disable**. The **no ppp multilink fragmentation** command was recognized and accepted through Cisco IOS Release 12.2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines   The ppp multilink fragment delay and ppp multilink interleave commands have precedence over the ppp multilink fragment disable command. Therefore, the ppp multilink fragment disable command has no effect if these commands are configured for a multilink interface and the following message displays:

```
Warning: 'ppp multilink fragment disable' or 'ppp multilink fragment maximum' will be
ignored, since multilink interleaving or fragment delay has been configured and have
higher precedence.
```

To completely disable fragmentation, you must do the following:

```
Router(config-if)# no ppp multilink fragment delay
Router(config-if)# no ppp multilink interleave
Router(config-if)# ppp multilink fragment disable
```

Disable multilink fragmentation using the **ppp multilink fragment disable** command if fragmentation causes performance degradation. Performance degradation due to multilink fragmentation has been observed with asynchronous member links.

Examples   The following example disables packet fragmentation:

```
ppp multilink fragment disable
```

Related Commands

Command	Description
ppp multilink fragment delay	Specifies a maximum size, in units of time, for packet fragments on an MLP bundle.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink mrru	Configures the Maximum Receive Reconstructed Unit (MRRU) value negotiated on a Multilink PPP (MLP) bundle.

ppp multilink group

To restrict a physical link to join only one designated multilink group interface, use the **ppp multilink group** command in interface configuration mode. To remove this restriction, use the **no** form of this command.

ppp multilink group *group-number*
no ppp multilink group

Syntax Description

group-number	Multilink group number (a nonzero number).

Command Default

If the **ppp multilink group** command is configured on an interface, the interface can join any multilink group. If the **ppp multilink group** command is not configured on an interface, the interface cannot join a multilink group.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0	This command was introduced as the **multilink-group** command on the PRE1 for the Cisco 10000 series router.
12.2	This command was changed to **ppp multilink group**. The **multilink-group** command is accepted by the CLI through Cisco IOS Release 12.2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was implemented on the PRE3 for the Cisco 10000 series router.
15.4(1)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

When the **ppp multilink group** command is configured on an interface, the interface is restricted from joining any interface but the designated multilink group interface. If a peer at the other end of the interface tries to join a different multilink group, the connection is severed. This restriction applies when Multilink PPP (MLP) is negotiated between the local end and the peer system. The link can still come up as a regular PPP interface.

The **ppp multilink group** command cannot be configured on an interface if the multilink group interface is not configured.

To modify the multilink group configuration on a serial interface, the existing PPP multilink group configuration must be removed from the serial interface.

When the multilink group interface is removed, the PPP multilink group configuration is removed from all the member links that have joined the specified multilink group.

The **ppp multilink group** command is primarily used with the MLP inverse multiplexer as described in the "Configuring Media-Independent PPP and Multilink PPP" chapter in the *Dial Technologies Configuration Guide*.

Cisco 10000 Series Router

The group-number option of the **ppp multilink group** command identifies the multilink group. This number must be identical to the multilink-bundle-number that you assign to a multilink interface. Valid group-number values are:

- MLP over serial-based Link Fragmentation and Interleaving (LFI)

    - 1 to 9999 (Cisco IOS Release 12.2(28)SB and later releases)
    - 1 to 2,147,483,647 (Cisco IOS Release 12.2(31)SB2 and later releases)

- Single-VC MLP over ATM-based LFI

    - 10,000 and higher

- Multi-VC MLP over ATM-based LFI

    - 1 to 9999 (Cisco IOS Release 12.2(28)SB and later releases)
    - 1 to 2,147,483,647 (Cisco IOS Release 12.2(31)SB2 and later releases)

- MLP over Frame Relay based LFI

    - 10,000 and higher

Examples

The following example shows how to configure a multilink group interface and configure a serial link to join the multilink group interface:

```
Router(config)# interface multilink 1
Router(config-if)# ip address 192.0.2.1 255.255.255.224
Router(config-if)# encapsulation ppp
Router(config-if)# exit
Router(config)# interface serial 1
Router(config-if)# encapsulation ppp
Router(config-if)# ppp multilink group 1
Router(config-if)# ppp multilink
Router(config-if)# exit
```

The following sample error message is displayed when a PPP multilink group is configured on a serial link before the multilink group interface is configured:

```
Router(config)# interface serial 2
Router(config-if)# ppp multilink group 1
% Multilink group interface does not exist. Please create a group interface first
```

The following sample error message is displayed when the multilink group configuration on a serial link is modified before the existing multilink group configuration is removed:

```
Router# show running-config interface serial4/0

Building configuration...

Current configuration : 188 bytes
!
interface Serial4/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
 ppp multilink fragment size 1000
 ppp multilink mrru local 1524
 serial restart-delay 0
end
Router# configure terminal
```

```
Router(config)# interface serial4/0
Router(config-if)# ppp multilink group 4
% Link is already part of Multilink1 group interface. Please detach it from the group
interface first.
```

The following sample output displays the serial interface configuration before and after the removal of the multilink group interface:

```
Router# show running-config interface serial5/0

Building configuration...
Current configuration : 188 bytes
!
interface Serial5/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
 ppp multilink fragment size 1000
 ppp multilink mrru local 1524
 serial restart-delay 0
end
Router# configure terminal
Router(config)# no interface Multilink 1
% Please 'shutdown' this interface before trying to delete it
Router(config)# interface Multilink 1
Router(config-if)# shutdown
Router(config-if)#
*Aug  2 17:35:11.825: %LINK-5-CHANGED: Interface Multilink1, changed state to administratively
 down
*Aug  2 17:35:11.826: %LINEPROTO-5-UPDOWN: Line protocol on Interface Multilink1, changed
state to down
*Aug  2 17:35:11.869: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial5/0, changed
state to down
*Aug  2 17:35:11.869: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial4/0, changed
state to down
Router(config-if)# exit
Router(config)#
*Aug  2 17:35:15.908: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial5/0, changed
state to up
*Aug  2 17:35:15.908: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial4/0, changed
state to up
Router(config)# no interface Multilink1
% The multilink group configuration will be removed from all the member links.
!
Router# show running-config interface serial5/0

Building configuration...
Current configuration : 165 bytes
!
interface Serial5/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink fragment size 1000
 ppp multilink mrru local 1524
 serial restart-delay 0
end
```

Related Commands	Command	Description
	encapsulation ppp	Enables PPP encapsulation on a serial interface.

Command	Description
interface multilink	Creates a multilink bundle or enters multilink interface configuration mode.
ip address	Configures an IP address for an interface.
ppp multilink	Enables an MLP on an interface.

ppp ncp override local

To track attributes received in authorization from RADIUS, verify the permitted Network Control Program (NCP), reject the current NCP negotiation, and override the local dual-stack configuration, use the **ppp ncp override local**command in global configuration mode. To disable the configuration, use the **no** form of this command.

ppp ncp override local
no ppp ncp override local

Syntax Description   This command has no arguments or keywords.

Command Default   The tracking of attributes from RADIUS and the local configuration override are not enabled. The local configuration is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines   Framed attributes are primarily used for address allocation. The RADIUS server maintains a pool of both IPv4 addresses and IPv6 prefixes. If IPv4 address or IPv6 prefix attributes are absent in the access-accept response from RADIUS, the **ppp ncp override local** command can be used to override local configuration.

Examples   The following example shows how to override the local IPv6 or IPv4 dual-stack configuration:

```
Router> enable

Router# configure terminal
Router(config)# ppp ncp override local
```

ppp timeout ncp

To set a time limit for the successful negotiation of at least one network layer protocol after a PPP connection is established, use the **ppp timeout ncp**command in interface configuration mode. To remove the time limit, use the **no** form of this command.

ppp timeout ncp *seconds*
no ppp timeout ncp

Syntax Description

seconds	Maximum time, in seconds, PPP should wait for negotiation of a network layer protocol. If no network protocol is negotiated in the given time, the connection is disconnected.

Command Default

No time limit is imposed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced as **ppp negotiation-timeout**.
12.2	This command was changed to **ppp timeout ncp**. The **ppp negotiation-timeout**command was accepted by the command line interpreter through Cisco IOS Release 12.2.
Cisco IOS XE Release 3.2S	Support for IPv6 was added.

Usage Guidelines

The **ppp timeout ncp** command protects against the establishment of links that are physically up and carrying traffic at the link level, but are unusable for carrying data traffic due to failure to negotiate the capability to transport any network level data. This command is particularly useful for dialed connections, where it is usually undesirable to leave a telephone circuit active when it cannot carry network traffic.

Examples

The following example sets the Network Control Protocol (NCP) timer to 8 seconds:

```
ppp timeout ncp 8
```

Related Commands

Command	Description
absolute-timeout	Sets the interval for closing user connections on a specific line or port.
dialer idle-timeout (interface)	Specifies the idle time before the line is disconnected.

ppp timeout ncp termination

To set a time limit for the successful renegotiation of at least one network layer protocol after a PPP connection is established, use the **ppp timeout ncp termination** command in interface configuration mode. To reset the default condition, use the **no** form of this command.

ppp timeout ncp *seconds* **termination** *seconds*
no ppp timeout ncp

Syntax Description

seconds	Maximum time, in seconds, PPP should wait for negotiation of a network layer protocol. If no network protocol is negotiated in the given time, the connection is disconnected.

Command Default   No time limit is imposed.

Command Modes   Interface configuration (config-if)

Command History

Release	Modification
12.2	This command was introduced.
Cisco IOS XE Release 3.2S	Support for IPv6 was added.

Usage Guidelines   The **ppp timeout ncp termination** command protects against the case where links are already established after negotiation of the network layer and later at some time if network layer gets terminated then this timer will be started and wait for the configured time period for renegotiation. This command is particularly useful for dialed connections, where it is usually undesirable to leave a telephone circuit active when it cannot carry network traffic.

Examples   The following example sets the Network Control Protocol (NCP) timer to ten seconds for negotiation of the network layer in the link establishment phase and one second for renegotiation after the network layer gets terminated at later time:

```
ppp timeout ncp 10 termination 1
```

Related Commands

Command	Description
absolute-timeout	Sets the interval for closing user connections on a specific line or port.
dialer idle-timeout (interface)	Specifies the idle time before the line is disconnected.

ppp unique address accept-access

To track duplicate addresses received from RADIUS and create a standalone database, use the **ppp unique address accept-access** command in global configuration mode. To disable this feature and remove the database, use the **no** form of this command.

ppp unique address accept-access
no ppp unique address accept-access

Syntax Description   This command has no arguments or keywords.

Command Default   This feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines   The ppp unique address accept-access command enables the IPv6 router to track and check duplicate attributes received in an Access-Accept response from RADIUS, and triggers creation of a new, standalone database that contains the Access-Accept responses received since the feature was enabled.

The following RADIUS attributes are tracked in this database and checked when an Access-Accept response is received:

- Framed-IP-Address

- Framed-IPv6-Prefix

- Delegated-IPv6-Prefix

All of these RADIUS attributes from this list are checked against the database for duplicates and, if none are found, added to the database exactly as presented in the RADIUS attribute.

Examples   The following example enables this feature:

```
Router (config)# ppp unique address accept-access
```

pppoe intermediate-agent format-type (global)

Note This command takes effect only if you enable the pppoe intermediate-agent global configuration command.

To set the access node identifier, generic error message, and identifier string for the switch, use the **pppoe intermediate-agent format-type** command. To disable the feature, use the **no** form of this command.

pppoe intermediate-agent format-type access-node-identifier string *string*
pppoe intermediate-agent format-type generic-error-message string *string*
pppoe intermediate-agent format-type identifier-string string *string* **option** {**sp** | **sv** | **pv** | **spv**} **delimiter**{**,** | **.** | **;** | **/** | **#**}
no pppoe intermediate-agent format-type {**access-node-identifier** | **generic-error-message** | **identifier-string**}

Syntax Description

access-node-identifier string *string*	ASCII string literal value for the access-node-identifier.
generic-error-message string *string*	ASCII string literal value for the generic-error-message.
identifier-string string *string*	ASCII string literal value for the identifier-string.
option {**sp**	**sv**	**pv**	**spv**}	Options: **sp** = slot + port **sv** = slot + VLAN **pv** = port + VLAN **spv** = slot + port + VLAN
delimiter {**,**	**.**	**;**	**/**	**#**}	Delimiter between slot/port/VLAN portions of **option**.

Command Default **access-node-identifier** has a default value of 0.0.0.0.

generic-error-message, **identifier-string**, **option**, and **delimiter** have no default values.

Command Modes Global configuration mode

Command History

Release	Modification
IOS XE 3.12	This command was implemented on Cisco ME 2600X switches.

Usage Guidelines Use the **access-node-identifier** and **identifier-string** commands t to enable the switch to generate the circuit-id parameters automatically.

The **no** form of identifier-string command resets the **option** and **delimiter**.

Use the **generic-error-message** command to set an error message notifying the sender that the PPPoE Discovery packet is too large

The following example shows how to set an access-node-identifier.

```
Device(config)# pppoe intermediate-agent format-type access-node-identifier string
```

The following example shows how to reset a generic-error-message.

```
Device(config)# no pppoe intermediate-agent format-type generic-error-message
```

Related Commands

Command	Description
show pppoe intermediate-agent info	Displays the PPPoE Intermediate Agent configuration.

pppoe intermediate-agent format-type (interface)

> **Note** This command takes effect only if you enable the pppoe intermediate-agent global and interface configuration command.

To set circuit-id or remote-id for an interface, use the **pppoe intermediate-agent format-type** command. To reset the parameters, use the **no** form of this command.

pppoe intermediate-agent format-type {circuit-id | remote-id}string*string*
nopppoe intermediate-agent format-type {circuit-id | remote-id}string*string*

Syntax Description

circuit-id string *string*	ASCII string literal value for circuit-id.
remote-id string *string*	ASCII string literal value for remote-id.

Command Default   No default values for circuit-id and remote-id.

Command Modes   Interface configuration mode

Command History

Release	**Modification**
IOS XE 3.12	This command was implemented on Cisco ME 2600X switches.

Usage Guidelines   Use the **pppoe intermediate-agent format-type** command to set interface-specific circuit-id and remote-id values. If an interface-specific circuit-id is not set, the system's automatic generated circuit-id value is used.

The following example shows how to set remote-id for an interface.

```
Device(config-if)# pppoe intermediate-agent format-type remote-id string user5451983
```

The following example shows how to reset circuit-id for an interface.

```
Device(config)# no pppoe intermediate-agent format-type circuit-id
```

Related Commands

Command	**Description**
pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.

pppoe intermediate-agent (global)

To enable the PPPoE Intermediate Agent feature on a switch, use the **pppoe intermediate-agent** global configuration command.. To disable the feature, use the **no** form of this command.

pppoe intermediate-agent
no pppoe intermediate-agent

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
IOS XE 3.12	This command was implemented on Cisco ME 2600X switches.

Usage Guidelines

You must enable PPPoE Intermediate Agent globally on a switch before you can use PPPoE Intermediate Agent on an interface or interface VLAN.

The following example shows how to enable PPPoE Intermediate Agent on a switch:

```
Device(config)# pppoe intermediate-agent
```

The following example shows how to disable PPPoE Intermediate Agent on a switch:

```
Device(config)# no pppoe intermediate-agent
```

Related Commands

Command	Description
pppoe intermediate-agent (global)	Sets the access node identifier, generic error message, and identifier string for a switch.

pppoe intermediate-agent (interface)

Note   This command takes effect only if you enable the **pppoe intermediate-agent** global command.

To enable the PPPoE Intermediate Agent feature on an interface, use the **pppoe enable** command. To disable the feature, use the **no** form of this command.

pppoe intermediate-agent
no pppoe intermediate-agent

Syntax Description   This command has no arguments or keywords.

Command Default   Disabled on all interfaces.

Command Modes   Interface configuration mode

Command History

Release	Modification
IOS XE 3.12	This command was implemented on Cisco ME 2600X switches.

Usage Guidelines   PPPoE Intermediate Agent is enabled on an interface provided the PPPoE Intermediate Agent is enabled both on the switch and the interface.

The following example shows how to enable the PPPoE Intermediate Agent on an interface:

```
Device(config-if)# pppoe intermediate-agent
```

The following example shows how to disable the PPPoE Intermediate Agent on an interface:

```
Device(config-if)# no pppoe intermediate-agent
```

Related Commands

Command	Description
pppoe intermediate-agent format-type (interface)	Sets circuit ID or remote ID for an interface.
pppoe intermediate-agent limit rate	Limits the rate of the PPPoE Discovery packets coming on an interface.
pppoe intermediate-agent trust	Sets the trust configuration of an interface.
pppoe intermediate-agent vendor-tag strip	Enables vendor-tag stripping on PPPoE Discovery packets from PPPoE Server (or BRAS).

pppoe intermediate-agent limit rate

To limit the rate of the PPPoE Discovery packets arriving on an interface, use the **pppoe intermediate-agent limit rate** command. To disable the feature, use the **no** form of this command.

pppoe intermediate-agent limit rate *number*
no pppoe intermediate-agent limit rate *number*

Syntax Description

number	Specifies the threshold rate of PPPoE Discovery packets received on this interface in packets-per-second.

Command Default

This command has no default settings.

Command Modes

Interface configuration mode

Command History

Release	Modification
IOS XE 3.12	This command was implemented on Cisco ME 2600X switches.

Usage Guidelines

If this command is used and the PPPoE Discovery packets that are received exceeds the rate set, the interface will be error-disabled (shutdown).

The following example shows how to set a rate limit for an interface:

```
Device(config-if)# pppoe intermediate-agent limit rate 40
```

The following example shows how to disable rate limiting for an interface:

```
Device(config-if)# no pppoe intermediate-agent limit rate
```

Related Commands

Command	Description
pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.

pppoe intermediate-agent trust

To set the trust configuration of an interface, use the **pppoe intermediate-agent trust** interface command. To reset the trust parameter, use the **no** form of this command.

pppoe intermediate-agent trust
no pppoe intermediate-agent trust

Syntax Description	This command has no arguments or keywords.
Command Default	All interfaces are untrusted.
Command Modes	Interface configuration mode

Command History

Release	Modification
IOS XE 3.12	This command was implemented on Cisco ME 2600X switches.

Usage Guidelines

At least one trusted interface must be present on the switch for PPPoE Intermediate Agent feature to work.

Set the interface connecting the switch to the PPPoE Server (or BRAS) as trusted.

The following example shows how to set an interface as trusted:

```
Device(config-if)# pppoe intermediate-agent trust
```

The following example shows how to disable the trust configuration for an interface:

```
Device(config-if)# no pppoe intermediate-agent trust
```

Related Commands

Command	Description
pppoe intermediate-agent vendor-tag strip	Enables vendor-tag stripping on PPPoE Discovery packets from a PPPoE Server (or BRAS).

pppoe intermediate-agent vendor-tag strip

Note This command takes effect only if you enable the **pppoe intermediate-agent interface configuration** command and the **pppoe intermediate-agent trust** command.

To enable vendor-tag stripping on PPPoE Discovery packets from PPPoE Server (or BRAS), use the **pppoe intermediate-agent vendor-tagstrip** command. To disable this setting, use the **no** form of this command.

pppoe intermediate-agent vendor-tag strip
no pppoe intermediate-agent vendor-tag strip

Syntax Description This command has no arguments or keywords.

Command Default vendor-tag stripping is turned off.

Command Modes Interface configuration mode

Command History

Release	Modification
IOS XE 3.12	This command was implemented on Cisco ME 2600X switches.

Usage Guidelines This command has no effect on untrusted interfaces.

Use this command on a PPPoE Intermediate Agent trusted interface to strip off the vendor-specific tags in PPPoE Discovery packets that arrive downstream from the PPPoE Server (or BRAS), if any.

The following example shows how to set vendor-tag stripping on an interface:

```
Device(config-if)# pppoe intermediate-agent vendor-tag strip
```

The following example shows how to disable vendor-tag stripping on an interface:

```
Device(config-if)# no pppoe intermediate-agent vendor-tag strip
```

Related Commands

Command	Description
pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.
pppoe intermediate-agent trust	Sets the trust configuration of an interface.

pppoe enable

To enable PPP over Ethernet (PPPoE) sessions on an Ethernet interface or subinterface, use the **pppoe enable** command in the appropriate configuration mode. To disable PPPoE, use the **no** form of this command.

pppoe enable [**group** *group-name*]
no pppoe enable

Syntax Description

group	(Optional) Specifies a PPPoE profile to be used by PPPoE sessions on the interface.
group-name	(Optional) Name of the PPPoE profile to be used by PPPoE sessions on the interface.

Command Default PPPoE is disabled by default.

Command Modes Interface configuration (config-if)

Subinterface configuration (config-subif)

VLAN configuration (vlan)

VLAN range configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(5)T	This command was modified to enable PPPoE on IEEE 802.1Q encapsulated VLAN interfaces.
12.2(15)T	The **group** keyword and the *group-name* argument were added.
12.3(2)T	This command was implemented in VLAN configuration mode and VLAN range configuration mode.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was implemented on the Cisco 10000 series routers.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

- If a PPPoE profile is not specified by using the **group** option, PPPoE sessions will be established using values from the global PPPoE profile.

- PPPoE profiles must be configured using the **bba-group pppoe** command.

Examples

PPPoE on an Ethernet Interface

The following example shows how to enable PPoE sessions on Ethernet interface 1/0. PPPoE sessions are established using the PPPoE parameters in the global PPPoE profile.

```
Device(config)# interface ethernet 1/0
Device(config-if)# pppoe enable
Device(config-if)# bba-group pppoe global
Device(config-bba-group)# virtual-template 1
Device(config-bba-group)# sessions max limit 8000
Device(config-bba-group)# sessions per-vc limit 8
Device(config-bba-group)# sessions per-mac limit 2
```

PPPoE on an 802.1Q VLAN Subinterface

The following example shows how to enable PPPoE on an 802.1Q VLAN subinterface. PPPoE sessions are established using the PPPoE parameters in PPPoE profile vpn1.

```
Device(config)# interface ethernet 2/3.1
Device(config-subif)# encapsulation dot1Q 1
Device(config-subif)# pppoe enable group vpn1
Device(config-subif)# bba-group pppoe vpn1
Device(config-bba-group)# virtual-template 1
Device(config-bba-group)# sessions per-vc limit 2
Device(config-bba-group)# sessions per-mac limit 1
```

PPPoE on an 802.1Q VLAN Main Interface

The following example shows how to configure PPPoE over a range of 802.1Q VLANs on Fast Ethernet interface 0/0. The VLAN range is configured on the main interface, and therefore each VLAN will not use up a separate subinterface.

```
Device(config)# interface fastethernet 0/0
Device(config-if)# no ip address
Device(config-if)# no ip mroute-cache
Device(config-if)# duplex half
Device(config-if)# vlan-range dot1q 20 30
Device(config-if-vlan-range)# pppoe enable group PPPOE
Device(config-if-vlan-range)# exit-vlan-config
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
debug pppoe	Displays debugging information for PPPoE sessions.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions permitted on a device and sets the PPPoE session-count threshold.
sessions per-vlan limit	Specifies the maximum number of PPPoE sessions in each VLAN.

pppoe limit max-sessions

Note   Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit max-sessions** command is replaced by the **sessions max limit** command. See the **sessions max limit** command for more information.

To specify the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on a router, use the **pppoe limit max-sessions** command in VPDN group configuration mode. To remove this specification, use the **no** form of this command.

pppoe limit max-sessions *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
no pppoe limit max-sessions

Syntax Description

number-of-sessions	Maximum number of PPPoE sessions that will be permitted on the router. The range is from 0 to the maximum number of interfaces on the router.
threshold-sessions	(Optional) Sets the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated.
number-of-sessions	(Optional) Number of PPPoE sessions that will cause an SNMP trap to be generated. The range is from 0 to the maximum number of interfaces on the router.

Command Default   The maximum number of sessions is not set.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was replaced by the **sessions max limit** command.

Usage Guidelines   PPPoE session limits configured using the **pppoe limit per-vc**, **pppoe limit per-vlan**, **pppoe max-sessions**, **pppoe max-sessions** (VC), and **pppoe max-sessions**(subinterface) commands take precedence over limits configured for the router using the **pppoe limit max-sessions** command.

Examples   The following example shows a limit of 100 PPPoE sessions configured for the router:

```
vpdn enable
vpdn-group 1
 accept dialin
```

```
 protocol pppoe
 virtual-template 1
pppoe limit max-sessions 100
```

Related Commands	**Command**	**Description**
	debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
	pppoe limit per-mac	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
	pppoe limit per-vc	Specifies the maximum number of PPPoE sessions permitted on all VCs.
	pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions permitted on a VLAN.
	pppoe max-sessions	Specifies the maximum number of PPPoE sessions permitted on an ATM PVC, PVC range, VC class, or Ethernet subinterface.

pppoe limit per-mac

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit per-mac** command is replaced by the **sessions per-mac limit** command. See the **sessions per-mac limit** command for more information.

To specify the maximum number of PPP over Ethernet (PPPoE) sessions to be sourced from a MAC address, use the **pppoe limit per-mac** command in VPDN configuration mode.

pppoe limit per-mac *number*

Syntax Description

number	Maximum number of PPPoE sessions that can be sourced from a MAC address.

Command Default 100 sessions

Command Modes

VPDN configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(28)SB	This command was replaced by the **sessions per-mac limit** command.

Examples The following example sets a limit of 10 sessions to be sourced from a MAC address:

```
pppoe limit per-mac 10
```

Related Commands

Command	Description
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions to be established over a VC.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions under each VLAN.

pppoe limit per-vc

✎

Note   Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit per-vc** command is replaced by the **sessions per-vc limit**command. See the **sessions per-vc limit** command for more information.

To specify the maximum number of PPP over Ethernet (PPPoE) sessions to be established over a virtual circuit (VC), use the **pppoe limit per-vc** command in VPDN configuration mode.

pppoe limit per-vc *number*

Syntax Description

number	Maximum number of PPPoE sessions that can be established over an ATM PVC.

Command Default   100 sessions

Command Modes

VPDN configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(28)SB	This command was replaced by the **sessions per-vc limit** command.

Examples   The following example sets a limit of 10 sessions to be established over a VC:

```
pppoe limit per-vc 10
```

Related Commands

Command	Description
pppoe limit max-sessions	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions under each VLAN.

pppoe limit per-vlan

✎

Note   Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit per-vlan** command is replaced by the **sessions per-vlan limit** command. See the **sessions per-vlan limit** command for more information.

To specify the maximum number of PPP over Ethernet (PPPoE) sessions permitted under each virtual LAN (VLAN), use the **pppoe limit per-vlan**command in VPDN configuration mode. To remove this specification, use the **no** form of this command.

pppoe limit per-vlan *number*
no pppoe limit per-vlan

Syntax Description

number	Maximum number of PPP over Ethernet sessions permitted under each VLAN.

Command Default   100 PPPoE sessions per VLAN

Command Modes

VPDN configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was replaced by the **sessions per-vlan limit** command.

Usage Guidelines   If the **pppoe max-session** command is configured on a VLAN, that command will take precedence over the **pppoe limit per-vlan** command. The **pppoe limit per-vlan** command applies to all VLANs on which the **pppoe max-session** command has not been configured.

The **pppoe limit per-vlan** command must be configured after the accept dial-in VPDN group has been configured using the **accept-dialin** VPDN configuration command.

Examples   The following example shows a maximum of 200 PPPoE sessions configured for an 802.1Q VLAN subinterface:

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 pppoe enable
!
vpdn enable
vpdn-group 1
 accept dialin
  protocol pppoe
  virtual-template 1
 pppoe limit per-vlan 200
```

Related Commands

Command	Description
accept dial-in	Creates an accept dial-in VPDN subgroup.
debug vpdn pppoe-data	Displays data packets of PPPoE sessions.
debug vpdn pppoe-error	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
debug vpdn pppoe-events	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
debug vpdn pppoe-packet	Displays each PPPoE protocol packet exchanged.
pppoe enable	Enables PPPoE sessions on an Ethernet interface.
pppoe limit max-sessions	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions to be established over a VC.
pppoe max-sessions	Specifies the maximum number of PPPoE sessions permitted under a VLAN.

pppoe max-sessions

To specify the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on an ATM permanent virtual circuit (PVC), PVC range, virtual circuit (VC) class, or Ethernet subinterface, use the **pppoe max-sessions** command in the appropriate mode. To remove this specification, use the **no** form of this command.

pppoe max-sessions *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
no pppoe max-sessions

Syntax Description

number-of-sessions	Maximum number of PPPoE sessions that will be permitted. The PPPoE sessions range depends on the device that you use. The range is 1 to 31992 on a Cisco 7200 series device.
	Note The PPPoE session limit in the case of a PVC range applies to *each* PVC in the range. This limit is not cumulative on *all* PVCs belonging to the range.
threshold-sessions	(Optional) Sets the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated.
number-of-sessions	(Optional) Number of PPPoE sessions that will cause an SNMP trap to be generated. The PPPoE sessions range depends on the device that you use. The range is 8500 to the maximum number specified for the PPPoE sessions on a Cisco 7200 series device.

Command Default

The maximum number of sessions is not set.

Command Modes

ATM PVC range configuration (config-if-atm-range)
ATM PVC-in-range configuration (config-if-atm-range-pvc)
ATM VC-class configuration (config-vc-class)
Ethernet subinterface configuration (config-if)
Interface-ATM-VC configuration (config-if-atm-vc)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(4)T	This command was modified to limit PPPoE sessions on ATM PVCs, PVC ranges, and VC classes.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC for Ethernet interfaces on the Cisco 7600 SIP-400.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

PPPoE sessions can be limited in the following ways:

- The **pppoe limit max-sessions**command limits the total number of PPPoE sessions on the router, regardless of the type of medium the sessions are using.

> **Note** Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit max-sessions** command is replaced by the **sessions max limit** command. See the **sessions max limit** command for more information.

- The **pppoe limit per-mac** command limits the number of PPPoE sessions that can be sourced from a single MAC address. This limit also applies to all PPPoE sessions on the router.

- The **pppoe limit per-vc** and **pppoe limit per-vlan**commands limit the number of PPPoE sessions on all PVCs or VLANs on the router.

- The **pppoe max-sessions** command limits the number of PPPoE sessions on a specific PVC or VLAN. Limits created for a specific PVC or VLAN using the **pppoe max-session** command take precedence over the global limits created with the **pppoe limit per-vc**and **pppoe limit per-vlan**commands.

PPPoE session limits created on an ATM PVC take precedence over limits created in a VC class or ATM PVC range.

Examples

Ethernet Subinterface Example

The following example shows a limit of 200 PPPoE sessions configured for the subinterface:

```
interface FastEthernet 0/0.10
 encapsulation dot1Q 10
 pppoe enable
 pppoe max-sessions 200
```

ATM PVC Example

The following example shows a limit of 10 PPPoE sessions configured for the PVC:

```
interface ATM1/0.102 multipoint
 pvc 3/304
 encapsulation aal5snap
 protocol pppoe
 pppoe max-sessions 10
```

VC Class Example

The following example shows a limit of 20 PPPoE sessions that will be permitted per PVC in the VC class called "main":

```
vc-class atm main
 pppoe max-sessions 20
```

ATM PVC Range Example

The following example shows a limit of 30 PPPoE sessions that will be permitted per PVC in the PVC range called "range-1":

```
interface atm 6/0.110 multipoint
 range range-1 pvc 100 4/199
 encapsulation aal5snap
 protocol ppp virtual-template 2
 pppoe max-sessions 30
```

Individual PVC Within a PVC Range Example

The following example shows a limit of 10 PPPoE sessions configured for "pvc1", which is part of the ATM PVC range called "range1":

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

Related Commands

Command	Description
debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
pppoe limit max-sessions	Specifies the maximum number of PPPoE sessions permitted on a router.
pppoe limit per-mac	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions permitted on all VCs.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions permitted on a VLAN.
sessions max limit	Specifies the maximum number of PPPoE sessions permitted on a router.

pppoe pads disable-ac-info

To prevent a device from sending the access concentrator (AC)-name and AC-cookie tags in the PPP over Ethernet (PPPoE) Active Directory Session (PADS) packet, use the **pppoe pads disable-ac-info** command in global configuration mode. To restore the default behavior of sending AC-name and AC-cookie tags in the PADS packet, use the **no** form of this command.

pppoe pads disable-ac-info
no pppoe pads disable-ac-info

Syntax Description   This command has no arguments or keywords.

Command Default   The device sends the AC-name and AC-cookie tags in the PADS packet.

Command Modes   Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.12S	This command was introduced.

Usage Guidelines   Use the **pppoe pads disable-ac-info** command to prevent a device from sending the AC-name (Tag type 0x0102) and AC-cookie tags (Tag type 0x0104) in the PADS packet. The command affects PADS packets that are sent only on newly configured PPPoE interfaces on the device after the command is configured globally. It does not affect the PADS packets sent on previously created PPPoE interfaces.

The 0x0102 AC-Name tag indicates a unique string that identifies the AC unit from all other units. It can be a combination of trademark, model, serial ID information, and a UTF-8 rendition of the MAC address of the device.

The 0x0104 AC-Cookie tag is used by the AC to help protect denial-of-service attacks. The AC may include this cookie tag in a PPoE Active Discovery Offer (PADO) packet. If a host receives this tag, it must be returned unmodified in the subsequent PPPoE Active Discovery Request (PADR.)

There are no prerequisites for this command configuration, and none of the PPP features are altered.

Example

The following example shows how to disable the PPPoE PADS AC-name and AC-cookie tags:

```
Device(config)# pppoe pads disable-ac-info
```

pppoe server circuit-id delay

To specify the delay based on the PPP over Ethernet (PPPoE) tag circuit ID client, use the**pppoe server circuit-id delay** command in BBA group configuration mode. To remove the delay, use the **no** form of this command.

pppoe server circuit-id delay *milliseconds* **string** [**contains**] *circuit-id-string*
no pppoe server circuit-id delay *milliseconds* **string** [**contains**] *circuit-id-string*

Syntax Description

milliseconds	Time in milliseconds for PPPoE Active Discovery Offer (PADO) delay. The time range is between 0 to 9999 milliseconds.
string	Specifies the circuit ID string.
contains	Specifies the partial string match that contains the remote ID string.
circuit-id-string	Circuit ID tag sent by Digital Subscriber Line Access Multiplexer (DSLAM) or the client in the PPPoE Active Discovery Initiation (PADI) packet. **Note** The value for the *circuit-id-string*argumentcan contain spaces when enclosed with double quotation marks (for example, circuit ATM1/ 0/ 0 VC 0/100).

Command Default

If no PADO delay is defined or matched, the PADO is transmitted without delay.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(33)SB3	This command was introduced.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.0(1)M	This command was integrated into Cisco IOS 15.0(1)M.

Usage Guidelines

Use the **pppoe server circuit-id delay** command to configure a PADO transmission delay per circuit ID. The PPPoE Smart Server Selection feature allows you to configure a specific PADO delay for a received PADI packet. The PADO delay establishes the order in which the Broadband Remote Access Servers (BRASs) respond to PADIs by delaying their responses to particular PADIs as per the delay time specified.

Examples

The following example shows how to configure PADO delay based on the circuit ID:

```
Router(config)# bba-group pppoe name1
Router(config-bba-group)# pppoe server circuit-id delay 20 string contains TEST

Router(config-bba-group)# pppoe server circuit-id delay 10 string XTH

Router(config-bba-group)# pppoe server circuit-id delay 30 string contains XTH-TEST

Router(config-bba-group)# pado delay 50
```

Generally, the first match found in the list is considered for the delay value. If the remote ID in the client PPPoE tag contains XTH-TEST, then the delay value is 20. In this case, the first match succeeds and the configuration never reaches a delay of 30. If the remote ID in the client PPPoE tag contains TH-no, then no match is found.

The following example shows how to match the circuit ATM1/ 0/ 0 VC 0/100 string by using a circuit ID or remote ID delay configured for the PPPoE server:

```
Router(config)# bba-group pppoe server-selection
Router(config-bba-group)# pppoe server circuit-id delay 45 string "circuit ATM1/0/0 VC
0/100"
Router(config-bba-group)# pado delay circuit-id 35
Router(config-bba-group)# pado delay 45
```

The following examples show the PADO delay configurations using circuit ID:

1. If the PADI has a circuit ID and a remote ID tag, and the BBA group on the server does not have a circuit ID or remote ID (matching or non-matching) configured, the value configured via **pado delay** *delay-value* is used.

Server example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1. If the PADI has a circuit ID tag and the BBA group on the server has a circuit ID configured, but they do not match, the value configured via **pado delay circuit-id** *delay-value* is used.

Server example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id delay 2222 string Ethernet1/0:T
Router(config-bba-group)#pppoe server circuit-id string contains TT
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1. If the BBA group on the server has a matching circuit ID configured (partial or strict), the per-circuit-id delay which is configured using the **delay** argument in the **pppoe server circuit-id delay** *value* string *circuit-id-string* command*:*

Server example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id delay 5555 string Ethernet1/0:S
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1. If the BBA group on the server has a matching circuit ID configured (partial or strict), and no delay value is configured for the circuit ID string, the PADO delay value configured with the **pado delay circuit-id** *delay-value* command is used.

Server example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id string Ethernet1/0:S
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1. If the delay value is configured as zero and "nvgen" is the delay string, the non-volatile generation (NVGEN) process is not executed on the delay string, only if you have not configured the delay while configuring the circuit ID.

2. If you configure both the partial and strict match strings for a circuit ID, the preference depends on the order in which they are encountered:

Server example:

```
Router(config)#bba-group pppoe 1
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#vendor-tag remote-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id delay 2222 string contains S
Router(config-bba-group)#pppoe server circuit-id delay 4444 string Ethernet1/0:S
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1. In the case of remote ID configurations, the behavior is the same as described earlier for circuit IDs. If both the remote ID and circuit ID are configured, preference is given to the circuit ID configuration.

2. If the PADO delay is found to be the maximum allowed value (9999 msec), the PADI is discarded as shown in the example:

```
Router(config)#bba-group pppoe 1
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#vendor-tag remote-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id delay 9999 string contains S
Router(config)#end
Router#show debug
PPPoE:
  PPPoE protocol events debugging is on
  PPPoE protocol errors debugging is on
```

Related Commands	**Command**	**Description**
	bba-group pppoe	Creates a PPPoE profile.
	pado delay	Establishes the order in which the BRASs respond to PADIs by delaying their responses to particular PADIs as per the delay time specified.
	pppoe server remote-id delay	Specifies the delay based on the PPPoE tag remote ID client.
	virtual template	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces.

pppoe server remote-id delay

To specify the delay to be applied on the PPP over Ethernet (PPPoE) tag remote ID client, use the **pppoe server remote-id delay** command in BBA group configuration mode. To remove the delay, use the **no** form of this command.

pppoe server remote-id delay *milliseconds* **string** [**contains**] *remote-id-string*
no pppoe server remote-id delay *milliseconds* **string** [**contains**] *remote-id-string*

Syntax Description

milliseconds	Time in milliseconds for the PPPoE Active Discovery Offer (PADO) delay.
string	Specifies the remote ID string.
contains	(Optional) Specifies the partial string match that contains the remote ID string.
remote-id-string	Remote ID tag sent by Digital Subscriber Line Access Multiplexer (DSLAM) or the client in the PPPoE Active Discovery Initiation (PADI) packet. **Note** The value for the *remote-id-string* argumentcan contain spaces when enclosed with double quotation marks (for example, subscr mac 1111.2222.3333).

Command Default

If no PADO delay is defined or matched, the PADO is transmitted without delay.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(33)SB3	This command was introduced.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS Release XE 2.4.
15.0(1)M	This command was integrated.

Usage Guidelines

The PPPoE Smart Server Selection feature allows you to configure a specific PADO delay for a received PADI packet. The PADO delay establishes the order in which the Broadband Remote Access Servers (BRASs) respond to PADIs by delaying their responses to particular PADIs by various times.

Use the **pppoe server remote-id delay** command to configure a PADO transmission delay per remote ID.

Examples

The following example shows how to configure PADO delay based on the remote ID:

```
Router(config)# bba-group pppoe name1
Router(config-bba-group)# pppoe server remote-id delay 20 string contains TEST

Router(config-bba-group)# pppoe server remote-id delay 10 string XTH
Router(config-bba-group)# pppoe server remote-id delay 30 string contains XTH-TEST

Router(config-bba-group)# pado delay 50
```

Generally, the first match found in the list is considered for the delay value. If the remote ID in the client PPPoE tag contains XTH-TEST, then the delay value is 20. In this case, the first match succeeds and the configuration never reaches a delay of 30. If the remote ID in the client PPPoE tag contains TH-no, then no match is found.

The following example shows how to match the subscr mac 1111.2222.3333 string by using a remote ID delay configured for PPPoE server:

```
Router(config)# bba-group pppoe server-selection
Router(config-bba-group)# pppoe server remote-id delay 45 string "subscr mac 1111.2222.3333"
Router(config-bba-group)# pado delay remote-id 35
```

Related Commands	Command	Description
	bba-group pppoe	Creates a PPPoE profile.
	pppoe server circuit-id delay	Specifies the delay based on the PPPoE tag circuit ID client.

pppoe service

To add a PPP over Ethernet (PPPoE) service name to a local subscriber profile, use the **pppoe service** command in subscriber profile configuration mode. To remove a PPPoE service name from a subscriber profile, use the **no** form of this command.

pppoe service *service-name*
no pppoe service *service-name*

Syntax Description

service-name	Name of the PPPoE service to be added to the subscriber profile.

Command Default

A PPPoE service name is not part of a subscriber profile.

Command Modes

Subscriber profile configuration (config-sss-profile)#

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE 2.3.0	This command was integrated. This command is supported on ASR 1000 series.

Usage Guidelines

A subscriber profile contains a list of PPPoE service names. Use the **pppoe service** command to add PPPoE service names to a local subscriber profile.

When you configure PPPoE service selection, you define a RADIUS service profile for each service name, list the service names that you want to advertise in a subscriber profile, and then assign the subscriber profile to a PPPoE profile. The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile.

Examples

The following example shows PPPoE service names being added to the subscriber profile called "listA":

```
!
! Configure the AAA default authorization method
aaa new-model
aaa authorization network default local
!
! Configure the subscriber profile
subscriber profile  listA
 pppoe service isp1
 pppoe service isp2
 pppoe service isp3
!
! Configure the PPPoE profile
bba-group pppoe group1
 virtual-template 1
 sessions per-vc  5
 service profile listA
!
```

```
! Attach the PPPoE profile to a PVC
interface atm1/0.1
 pvc 2/200
 protocol PPPoE group1
!
```

Related Commands

Command	Description
clear pppoe derived	Clears the cached PPPoE configuration of a PPPoE profile and forces the PPPoE profile to reread the configuration from the assigned subscriber profile.
service profile	Assigns a subscriber profile to a PPPoE profile.
show pppoe derived	Displays the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.
subscriber profile	Defines Subscriber Service Switch policy for searches of a subscriber profile database.

pppoe-sessions threshold

To configure the per-physical interface threshold value of the Cisco ASR 1000 Series Aggregation Services Routers, use the **pppoe-sessions threshold** command in interface configuration mode. To disable the threshold value, use the **no** form of this command.

pppoe-sessions threshold *number*
no pppoe-sessions threshold *number*

Syntax Description

| *number* | Maximum number of permissible PPPoE sessions. Range: 1 to 65535. |

Command Default

The per-physical interface threshold value is not set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following example shows how to configure 90 PPPoE sessions as the per-physical threshold value on the Cisco ASR 1000 Series Router:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0
Router(config-if)# pppoe-sessions threshold 90
```

Related Commands

Command	Description
sessions threshold	Configures the global threshold value of the PPPoE session on the Cisco ASR1000 Series Router.

protocol pppoe (ATM VC)

To enable PPP over Ethernet (PPPoE) sessions to be established on permanent virtual circuits (PVCs), use the **protocol pppoe** command in the appropriate configuration mode. To disable PPPoE, use the **no** form of this command.

protocol pppoe [{**group** *group-name* | **global**}]
no protocol pppoe [{**group** *group-name* | **global**}]

Syntax Description

group	(Optional) Specifies a PPPoE profile to be used by PPPoE sessions on the interface.
group-name	(Optional) Name of the PPPoE profile to be used by PPPoE sessions on the interface.
global	(Optional) Specifies a global PPPoE profile to be used by PPPoE sessions on the interface.

Command Default

PPPoE is not enabled.

Command Modes

ATM PVC-in-range configuration (cfg-if-atm-range-pvc)
ATM PVC range configuration (config-if-atm-range)
ATM VC class configuration (config-vc-class)
ATM VC configuration (config-if-atm-vc)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

If a PPPoE profile is not specified by using the **group** option, PPPoE sessions will be established using values from the global PPPoE profile. PPPoE profiles must be configured using the **bba-group pppoe** command.

Examples

The following example shows PPPoE configured in virtual circuit (VC) class "class-pppoe-global" and on the range of PVCs from 100 to 109. PVCs that use VC class "class-pppoe-global" will establish PPPoE sessions using the parameters configured in the global PPPoE profile. PVCs in the PVC range will use PPPoE parameters defined in PPPoE profile "vpn1".

```
bba-group pppoe global
 virtual-template 1
 sessions max limit 8000
 sessions per-vc limit 8
 sessions per-mac limit 2
!
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 2
```

```
 sessions per-mac limit 1
!
vc-class atm class-pppoe-global
 protocol pppoe
!
interface ATM1/0.10 multipoint
 range range-pppoe-1 pvc 100 109
  protocol pppoe group vpn1
 !
interface ATM1/0.20 multipoint
 class-int class-pppoe-global
 pvc 0/200
!
 pvc 0/201
 !
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
debug pppoe	Displays debugging information for PPPoE sessions.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions permitted on a router and sets the PPPoE session-count threshold.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC and sets the PPPoE session-count threshold.

protocol pppovlan dot1q

To configure an ATM PVC to support PPPoE over a specific IEEE 802.1Q VLAN or range of VLANs, use the **protocol pppovlan dot1q** command in ATM VC configuration or VC class configuration mode. To disable ATM PVC support for PPPoE for a specific IEEE 802.1Q VLAN or a range of VLANs, use the **no** form of this command.

protocol pppovlan dot1q {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]
no protocol pppovlan dot1q {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]

Syntax Description

vlan-id	VLAN identifier. Valid values range from 1 to 4095.
start-vlan-id	VLAN identifier of the first VLAN in the range. Valid values range from 1 to 4095.
end-vlan-id	VLAN identifier of the last VLAN in the range. Valid values range from 1 to 4095.
group	(Optional) Specifies that a PPPoE profile will be used by PPPoE sessions on the interface.
group-name	(Optional) Name of the PPPoE profile to be used by PPPoE sessions on the interface.

Command Default

ATM PVC support for PPPoE over 802.1Q VLAN encapsulation is not enabled.

Command Modes

ATM VC configuration
VC class configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB

Usage Guidelines

The **protocol pppovlan dot1q** command enables an ATM PVC to support PPPoE over 802.1Q VLAN traffic that uses bridged RFC 1483 encapsulation.

An ATM PVC will drop 802.1Q traffic that is configured for non-PPPoE VLANs.

PPPoE over 802.1Q VLANs over ATM is supported on the PPPoE server only.

Examples

The following example shows how to configure an ATM PVC to support PPPoE over a range of 802.1Q VLANs:

```
bba-group pppoe PPPOEOA
 virtual-template 1
 sessions per-mac limit 1
interface virtual-template 1
 ip address 10.10.10.10 255.255.255.0
 mtu 1492
interface atm 4/0.10 multipoint
```

```
pvc 10/100
 protocol pppovlan dot1q 10 30 group PPPOEOA
```

Related Commands

Command	Description
debug pppoe	Displays debugging information for PPPoE sessions.

provision code

To specify the provision code to be used by the customer premise equipment (CPE), use the **provision code** command in TR-069 Agent configuration mode.

provision code *code-string*

Syntax Description

code-string	The provision code.

Command Modes

TR-069 Agent configuration (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to specify the provision code to be used by the CPE:

```
Device(config-cwmp)# provision code ABCD
```

pvc-in-range

To configure an individual permanent virtual circuit (PVC) within a PVC range, use the **pvc-in-range** command in PVC range configuration mode. To delete the individual PVC configuration, use the **no** form of this command.

pvc-in-range[{*pvc-name*}][{*vpi/vci*}]
no pvc-in-range[{*pvc-name*}][{*vpi/vci*}]

Syntax Description

pvc-name	(Optional) Name given to the PVC. The PVC name can have a maximum of 15 characters.
vpi /	(Optional) ATM network virtual path identifier (VPI) for this PVC. In the absence of the "/" and a *vpi* value, the *vpi* value defaults to 0. The *vpi* value ranges from 0 to 255.
vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. The *vci* value ranges from 32 to 2047.

Command Default

No default behavior or values

Command Modes

PVC range configuration (config-if-atm-range)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

The **pvc-in-range** command defines an individual PVC within a PVC range and enables PVC-in-range configuration mode.

Examples

In the following example, a PVC called "pppoa" is deactivated. The PVC "pppoa" is an individual PVC within a configured PVC range.

```
pvc-in-range pppoa 0/130
 shutdown
```

Related Commands

Command	Description
range pvc	Defines a range of ATM PVCs.

radius-server vsa send

To configure the network access server (NAS) to recognize and use vendor-specific attributes (VSAs), use the **radius-server vsa send**command in global configuration mode. To restore the default, use the **no**form of this command.

radius-server vsa send [{**accounting** | **authentication** | **cisco-nas-port**}] [**3gpp2**]
no radius-server vsa send [{**accounting** | **authentication** | **cisco-nas-port**}] [**3gpp2**]

Syntax Description

accounting	(Optional) Limits the set of recognized VSAs to only accounting attributes.
authentication	(Optional) Limits the set of recognized VSAs to only authentication attributes.
cisco-nas-port	(Optional) Due to the Internet Engineering Task Force (IETF) requirement for including NAS port information in attribute 87 (Attr87), the Cisco NAS port is obsoleted by default. However, if your servers require this information, then the **cisco-nas-port** keyword can be used to return the Cisco NAS port VSA.
3gpp2	(Optional) Adds Third Generation Partnership Project 2 (3gpp2) Cisco VSAs to this packet type.

Command Default NAS is not configured to recognize and use VSAs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **cisco-nas-port** and **3gpp2** keywords were added to provide backward compatibility for Cisco VSAs.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S.	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines The IETF draft standard specifies a method for communicating vendor-specific information between the NAS and the RADIUS server by using the VSA (attribute 26). VSAs allow vendors to support their own extended attributes not suitable for general use. The **radius-server vsa send**command enables the NAS to recognize and use both accounting and authentication VSAs. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to accounting attributes only. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to authentication attributes only.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string with the following format:

```
protocol : attribute sep value *
```

In the preceding example, "protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; "attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification; and "sep" is "=" for mandatory attributes and "*" for optional attributes. This solution allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes the Cisco "multiple named ip address pools" feature to be activated during IP authorization (during the PPP Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example causes a "NAS Prompt" user to have immediate access to EXEC commands.

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, see RFC 2138, Remote Authentication Dial-In User Service (RADIUS).

Examples

The following example shows how to configure the NAS to recognize and use vendor-specific accounting attributes:

```
Router(config)# radius-server vsa send accounting
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-Port attribute with RADIUS IETF attribute 26 and displays extended field information.

range pvc

To define a range of ATM permanent virtual circuits (PVCs), use the **range pvc** command in interface configuration mode or subinterface configuration mode. To delete the range of ATM PVCs, use the **no** form of this command.

range{[*rangem-name*]} *start-vci*[{*end-vpi/*}]*end-vci*
no range [*range-name*] **pvc**

Syntax Description

range-name	(Optional) Name of the range. The range name can be a maximum of 15 characters.
start-vpi /	(Optional) Beginning value for a range of virtual path identifiers (VPIs). In the absence of the "/" and a *vpi* value, the *vpi* value defaults to 0. The *vpi* value ranges from 0 to 255.
start-vci /	Beginning value for a range of virtual channel identifiers (VCIs). The *vci* value ranges from 32 to 65535.
end-vpi /	(Optional) End value for a range of virtual path identifiers (VPIs). In the absence of an *end-vpi* value, the *end-vpi* value defaults to the *start-vpi* value. The *vpi* value ranges from 0 to 255.
end-vci	End value for a range of virtual channel identifiers (VCIs). The *vci* value ranges from 32 to 65535.

Command Default

An ATM PVC range is not configured.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

The **range pvc**command defines a range of PVCs and enables PVC range configuration mode.

The number of PVCs in a range can be calculated using the following formula:

number of PVCs = (*end-vpi* - *start-vpi* + 1) x (*end-vci* - *start-vci* +1).

The *start-vpi* argument may be omitted if it is zero. The *end-vpi* argument may be omitted, but if it is omitted, it is assigned the value of *start-vpi* . The *end-vpi* and *end-vci* arguments are always greater than or equal to *start-vpi* and *start-vci* respectively.

When applied to multipoint subinterfaces, the **range pvc** command creates a range of ATM PVCs. When applied to point-to-point subinterfaces, the **range pvc** command creates range of PVCs and a corresponding range of point-to-point subinterfaces.

For point-to-point subinterfaces, subinterface numbering begins with the subinterface on which the PVC range is configured and increases sequentially through the range.

Examples

ATM PVC Range Example

In the following example, 100 PVCs with VCI values from 100 to 199 for each VPI value from 0 to 4 are created for a PVC range called "range-pppoa-1". This configuration creates a total of 500 PVCs in the range. PVC parameters are then configured for the range.

```
interface atm 6/0.110 multipoint
 range range-pppoa-1 pvc 100 4/199
  class-range class-pppoa-1
  ubr 1000
  encapsulation aal5snap
  protocol ppp virtual-Template 2
```

Subinterface Grouping by PVC Range for Routed Bridge Encapsulation Example

In the following example, a PVC range called "range1" is created with a total of 100 PVCs in the range. A point-to-point subinterface will be created for each PVC in the range. ATM routed bridge encapsulation is also configured.

```
interface atm 6/0.200 point-to-point
 ip unnumbered loopback 1
 atm route-bridged ip
 range range1 pvc 1/200 1/299
  # end
```

Related Commands

Command	Description
pvc-in-range	Configures an individual PVC within a PVC range.

rbe nasip

To specify the IP address of an interface on the DHCP relay agent that will be sent to the DHCP server via the agent remote ID option, use the **rbe nasip** command in global configuration mode. To remove the specification, use the **no** form of this command.

rbe nasip *interface-type number*
no rbe nasip

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

No IP address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

The **rbe nasip** command is used to configure support for the DHCP relay agent information option (option 82) for an ATM routed bridge encapsulation (RBE).

Support for the DHCP relay agent information option must be configured on the DHCP relay agent using the **ip dhcp relay information option** command for the **rbe nasip** command to be effective.

Examples

The following example shows how to enable support for DHCP option 82 on the DHCP relay agent by using the **ip dhcp relay information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server. ATM RBE is configured on ATM subinterface 4/0.1.

```
ip dhcp-server 10.1.1.1
!
ip dhcp relay information option
!
interface Loopback0
 ip address 10.5.1.1 255.255.255.0
!
interface ATM 4/0
 no ip address
!
interface ATM 4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 10.1.1.1
```

```
 atm route-bridged ip
 pvc 88/800
  encapsulation aal5snap
!
router eigrp 100
 network 10.0.0.0
!
rbe nasip loopback 0
```

Related Commands

Command	Description
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.

relay pppoe bba-group

To configure the PPP over Ethernet (PPPoE) broadband access (BBA) group that responds to PPPoE Active Discovery (PAD) messages, use the **relay pppoe bba-group** command in VPDN group or VPDN template configuration mode. To unconfigure the group, use the **no** form of this command.

relay pppoe bba-group *pppoe-bba-group-name*
no relay pppoe bba-group *pppoe-bba-group-name*

Syntax Description

pppoe-bba-group-name	Name of the PPPoE BBA group.

Command Default
No PPPoE BBA group is configured to respond to PAD messages.

Command Modes

VPDN group configuration
VPDN template configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines
On the router that responds to relayed PAD messages, this command configures a PPPoE group and attaches it to a virtual private dialup network (VPDN) group or VPDN template that accepts dial-in calls for Layer 2 Tunnel Protocol (L2TP). The relayed PAD messages will be passed from the VPDN L2TP tunnel or session to the PPPoE broadband group for receiving the PAD response.

Examples
The following partial example shows how to configure a tunnel switch or L2TP tunnel server to respond to PAD messages. The **relay pppoe bba-group** command configures PPPoE "group-1", which is attached to accept dial-in VPDN group "Group-A".

```
.
.
.
vpdn-group Group-A
! Configure an L2TP tunnel for PPPoE Relay
 accept-dialin
  protocol l2tp
.
.
.
 terminate-from hostname LAC-1
 relay pppoe bba-group group-1
.
.
.
! Configure the PPPoE group to respond to the relayed PAD messages
bba-group pppoe group-1
 service profile profile-1
```

Related Commands	Command	Description
	bba-group pppoe	Creates a PPPoE profile.
	vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
	vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

request outstanding

To set the count for the number of requests that can be sent by the customer premise equipment (CPE) to the auto-configuration server (ACS) without receiving an acknowledgement, use the **request outstanding** command in TR-069 Agent configuration mode.

request outstanding *request-count*

Syntax Description

request-count	The count for the number of requests. The range for the request count is 0 to 10. The default value is 5.

Command Default

The count is set to 5.

Command Modes

TR-069 Agent configuration (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to set the count to 6 for the number of requests that can be sent by the CPE to the ACS without receiving an acknowledgement:

```
Device(config-cwmp)# request outstanding 6
```

rx-speed

To configure the required speed on the ATM virtual circuit (VC) carrying the PPPoX session, and to transfer this information into attribute-value (AV) pair 38 from the Layer 2 Tunnel Protocol (L2TP) Access Concentrator (LAC) to the L2TP network server (LNS) for asymmetric digital subscriber line (DSL) sessions, use the **rx-speed** command in PVC class, PVC-in-range, or PVC range configuration mode. To reset the variable to have the same value as that passed in AVP 24, use the **no** form of this command.

rx-speed *incoming-cell-rate*
no rx-speed

Syntax Description

incoming-cell-rate	Incoming cell rate for L2TP AVP 38, in kb/s.

Command Default

The same value as that passed in AVP 24.

Command Modes

PVC-class (config-if-atm-vc)
PVC-in-range (cfg-if-atm-range-pvc)
PVC range (config-if-atm-range)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

To allow L2TP to send AVP 38 with the required value from LAC to LNS for DSL services, use the **rx-speed** command in PVC, PVC-in-range, or PVC range configuration mode.

The configured speed is transported to the LNS, which validates the session within AVP 24 and AVP 38.

Examples

The following examples show how L2TP sends AVP 38 with the required value to the LNS in PVC-class, PVC range, and PVC-in-range configuration modes:

PVC-class

```
Router(config)# interface atm 6/0.110 multipoint
Router(config-subif)# pvc 0/600
Router(config-if-atm-vc)# rx-speed 128
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# exit
```

PVC-in-Range

```
Router(config)# interface atm 6/0.110 multipoint
Router(config-subif)# range range1 pvc 100 4/199
```

rx-speed

```
Router(config-if-atm-range)# pvc-in-range 0/300 45/54
Router(cfg-if-atm-range-pvc)# rx-speed 200
Router(cfg-if-atm-range-pvc)# shutdown
```

PVC Range

```
Router(config)# interface atm 6/0.110 multipoint
Router(config-subif)# range range-pppoa-1 pvc 100 4/199
Router(config-if-atm-range)# rx-speed 400
Router(config-if-atm-range)# exit
```

Related Commands	**Command**	**Description**
	encapsulation (ATM)	Configures the AAL and encapsulation type for an ATM VC, VC class, VC, bundle, or PVCs.
	pvc	Creates or assigns a name to an ATM PVC, to specify the encapsulation type on an ATM PVC, and to enter ATM VC configuration mode.
	pvc-in-range	Configures an individual PVC within a PVC range.
	range pvc	Defines a range of ATM PVCs.

service deny

To deny service for the Subscriber Service Switch (SSS) policy, use the **service deny**command in subscriber profile configuration mode. To remove the configuration, use the **no** form of this command.

service deny
no service deny

Syntax Description   This command has no arguments or keywords.

Command Default   This command is disabled by default.

Command Modes

Subscriber profile configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines   The **service deny** command denies service to a subscriber for the SSS policy defined with the **subscriber profile**command..

Examples   The following example denies service to users in the domain cisco.com:

```
!
subscriber profile cisco.com
 service deny
```

Related Commands

Command	Description
service local	Enables local termination service for the SSS policy.
service relay	Enables relay of PAD messages over an L2TP tunnel.
service vpdn group	Provides VPDN service for the SSS policy.
subscriber profile	Defines the SSS policy for searches of a subscriber profile database.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.

service local

To define local termination service for the Subscriber Service Switch (SSS) policy, use the **service local**command in subscriber profile configuration mode. To remove the service, use the **no** form of this command.

service local
no service local

Syntax Description   This command has no arguments or keywords.

Command Default   This command is enabled by default.

Command Modes

Subscriber profile configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines   The **service local**command is used to configure local termination service for the SSS policy defined with the **subscriber profile**command.

Examples   The following example provides local termination service to users in the domain cisco.com:

```
!
subscriber profile cisco.com
 service local
```

Related Commands

Command	Description
service deny	Denies service for the SSS policy.
service relay	Enables relay of PAD messages over an L2TP tunnel.
service vpdn group	Provides VPDN service for the SSS policy.
subscriber profile	Defines the SSS policy for searches of a subscriber profile database.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.

service name match

To force the Point to Point Protocol over Ethernet (PPPoE) server to match the service name received in the PPPoE Active Discovery Initiation (PADI) message, use the **service name match** command in BBA group configuration mode. To disable the configuration, use the **no** form of this command.

service name match
no service name match

Syntax Description   This command has no arguments or keywords.

Command Default   No services are configured.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(33)SB	This command was introduced.

Usage Guidelines   This command forces the PPPoE server to match the service-name received in the PADI message from the PPPoE client, to one of the PPPoE service names in the policy map type service list with its name configured as service profile before it responds. When a match is found, a Point Protocol over Ethernet Active Discovery Offer (PADO) message is returned to the PPPoE client in response to the PADI message received.

Examples   The following example illustrates service name match configuration:

```
Router(config)# bba-group pppoe
 name1
Router(config-bba-group)# service profile
 list1
Router(config-bba-group)# service name match
Router(config-bba-group)# policy-map type service
 list1
Router(config-bba-group)# pppoe service name
Router(config-bba-group)# pppoe service name1
The following example illustrates how the PPPoE service profile is configured. The service
 name match requires the requested service to match either service-1 or another-service:
Router(config)# bba-group pppoe
 name1
Router(config-bba-group)# service profile
 list1
Router(config-bba-group)# service name match
Router(config-bba-group)# policy-map type service
 list1
Router(config-bba-group)# pppoe service
 service-1
Router(config-bba-group)# pppoe service
 another-service
```

Related Commands

Command	Description
pppoe service	Adds a PPPoE service name to a local subscriber profile.
bba-group pppoe	Creates a PPPoE profile
policy-map type service	Creates or modifies a service policy map, which is used to define an ISG subscriber service.

service netflow timeout

To configure NetFlow PXF timers for active and inactive flow entries in the Cisco IOS NetFlow cache on the Cisco 10000 series router, use the s**ervice netflow timeout**command in global configuration mode.

service netflow timeout [{**active** | **inactive**}] *value*

Syntax Description

active	Specifies the NetFlow PXF timeout for active flow entries.
inactive	Specifies the NetFlow PXF timeout for inactive flow entries.
value	Specifies the NetFlow PXF timeout, in seconds. Range is from 0 to 4292967295.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB2	This command was introduced in Cisco IOS Release 12.2(28)SB2 and implemented on the Cisco 10000 series router.

Usage Guidelines

This command is not supported for customer use without Cisco Technical Assistance Center (TAC) authorization.

If you configure the timers, the router does not retain your settings on PXF or Performance Routing Engine (PRE) reloads. On PXF and PRE reloads, the active timeout reverts to 60 seconds and the inactive timeout to 15 seconds.

We recommend that the active timeout value be larger than the inactive timeout value. Also, we recommend that you do not configure the inactive timeout lower than 15 seconds to prevent the sending of excessive flow records from the PXF to the Route Processor (RP).

The service internal command is required to configure the NetFlow PXF timers.

Examples

The following example shows how to set the NetFlow PXF active timeout to 90 seconds:

```
Router> enable
Router# configure terminal
Router(config)# service internal
Router(config)# service netflow timeout active 90
Router(config)# end
```

Related Commands

Command	Description
show ip cache flow	Displays a summary of NetFlow accounting statistics.

service profile

To assign a subscriber profile to a PPP over Ethernet (PPPoE) profile, use the **service profile** command in BBA group configuration mode. To remove a subscriber profile assignment from a PPPoE profile, use the **no** form of this command.

service profile *subscriber-profile-name* [**refresh** *minutes*]
no service profile *subscriber-profile-name* [**refresh** *minutes*]

Syntax Description

subscriber-profile-name	Name of the subscriber profile to be assigned to a PPPoE profile.
refresh	(Optional) Causes the cached PPPoE configuration to be timed out and reread from the subscriber profile.
minutes	Number of minutes after which the cached PPPoE configuration will be timed out. The range is from 2 to 44640 minutes. There is no default.

Command Default
A subscriber profile is not assigned to a PPPoE profile.

Command Modes

BBA group configuration (config-bba-group)#

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE 2.3.0	This command was integrated. This command is supported on ASR 1000 series.

Usage Guidelines
A subscriber profile contains a list of PPPoE service names. Use the **service profile** command to assign a subscriber profile to a PPPoE profile. The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile.

A subscriber profile can be configured locally on the router or remotely on a AAA server. The PPPoE configuration that is derived from a subscriber profile is cached locally under the PPPoE profile. Use the **service profile** command with the **refresh** keyword and the *minutes* argument to cause the cached PPPoE configuration to be timed out after a specified number of minutes. When the cached PPPoE configuration is timed out, the PPPoE profile rereads the configuration in the subscriber profile.

Examples
The following example shows how to assign a subscriber profile called "customer_tunnels" to a PPPoE profile called "group_A":

```
!
! Configure the AAA default authorization method
aaa new-model
aaa authorization network default group radius
!
! Configure the PPPoE profile
bba-group pppoe group_A
 virtual-template 1
 sessions per-vc  5
```

```
 service profile customer_tunnels
!
! Attach the PPPoE profile to PVCs
interface atm1/0.1
 pvc 2/200
  protocol PPPoE group pppoe_group_A
!
interface atm1/0.2
 pvc 3/300
  protocol PPPoE group pppoe_group_A
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
clear pppoe derived	Clears the cached PPPoE configuration of a PPPoE profile and forces the PPPoE profile to reread the configuration from the assigned subscriber profile.
service profile	Assigns a subscriber profile to a PPPoE profile.
show pppoe derived	Displays the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.
subscriber profile	Defines Subscriber Service Switch policy for searches of a subscriber profile database.

service relay

To enable relay of PPPoE Active Discovery (PAD) messages over a Layer 2 Tunnel Protocol (L2TP) tunnel, use the **service relay**command in subscriber profile configuration mode. To disable message relay, use the **no** form of this command.

service relay pppoe vpdn group *vpdn-group-name*
no service relay pppoe vpdn group *vpdn-group-name*

Syntax Description

pppoe	Provides relay service using PPP over Ethernet (PPPoE) using a virtual private dialup network (VPDN) L2TP tunnel for the relay.
vpdn group *vpdn-group-name*	Provides VPDN service by obtaining the configuration from a predefined VPDN group.

Command Default

This command is disabled by default.

Command Modes

Subscriber profile configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **service relay**command is configured as part of a subscriber profile. The subscriber profile name is obtained based on the authorization key specified in the **service profile**PPPoE broadband access (BBA) group configuration command. See the "Examples" section for clarification.

Examples

The following example configures the group named Sample1.net to contain outgoing tunnel information for the relay of PAD messages over an L2TP tunnel:

```
subscriber profile profile-1
! Configure profile for PPPoE Relay
 service relay pppoe vpdn group Sample1.net
!
bba-group pppoe group-1
 virtual-template 1
 service profile profile-1
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
service	Configures the type of service that will be granted to a subscriber.
service profile	Assigns a subscriber profile to a PPPoE profile.

Command	Description
subscriber profile	Defines the SSS policy for searches of a subscriber profile database.

sessions threshold

To configure the global threshold value of PPP over Ethernet (PPPoE) sessions on the Cisco ASR 1000 Series Aggregation Services Router, use the **sessions threshold** command in BBA group configuration mode. To disable the global threshold value, use the **no** form of this command.

sessions threshold *number*
no sessions threshold *number*

Syntax Description

number	Maximum number of permissible PPPoE sessions. Range: 1 to 65535.

Command Default

The global threshold value is not set.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following example shows how to configure 1000 PPPoE sessions as the global threshold value on the **Cisco**ASR 1000 router:

```
Router# configure terminal
Router(config)# bba-group pppoe global
Router(config-bba-group)# sessions threshold 1000
```

Related Commands

Command	Description
pppoe-sessions threshold	Configures the per-physical interface threshold value of the ASR1000 router.

service vpdn group

To provide virtual private dialup network (VPDN) service for the Subscriber Service Switch policy, use the **service vpdn group** command in subscriber profile configuration mode. To remove VPDN service, use the **no** form of this command.

service vpdn group *vpdn-group-name*
no service vpdn group *vpdn-group-name*

Syntax Description

vpdn-group-name	Provides the VPDN service by obtaining the configuration from a predefined VPDN group.

Command Default   This command is disabled by default.

Command Modes   Subscriber profile configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines   The **service vpdn group** command provides VPDN service by obtaining the configuration from a predefined VPDN group for the SSS policy defined with the **subscriber profile** command.

Examples   The following example provides VPDN service to users in the domain cisco.com and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile cisco.com
 service vpdn group 1
```

The following example provides VPDN service to dialed number identification service (DNIS) 1234567 and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile dnis:1234567
 service vpdn group 1
```

The following example provides VPDN service using a remote tunnel (used on the multihop node) and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile host:lac
 service vpdn group 1
```

Related Commands

Command	Description
service deny	Denies service for the SSS policy.
service local	Enables local termination service for the SSS policy.

Command	Description
service relay	Enables relay of PAD messages over an L2TP tunnel.
subscriber profile	Defines the SSS policy for searches of a subscriber profile database.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.

sessions max limit

To configure the PPP over Ethernet (PPPoE) global profile with the maximum number of PPPoE sessions that will be permitted on a router and to set the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated, use the **sessions max limit**command in BBA group configuration mode. To remove these settings, use the **no** form of this command.

sessions max limit *number-of-sessions* [**threshold** *number-of-sessions*]
no sessions max limit *number-of-sessions* [**threshold** *number-of-sessions*]

Syntax Description

number-of-sessions	Maximum number of PPPoE sessions that will be permitted on the router. The range is from 0 to the total number of interfaces on the router.
threshold	(Optional) Sets the PPPoE session-count threshold at which an SNMP trap will be generated.
number-of-sessions	(Optional) Number of PPPoE sessions that will cause an SNMP trap to be generated. The range is from 0 to the total number of interfaces on the router.

Command Default

There is no default number of sessions. The default threshold value is the configured number of sessions.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

This command can be used only in a global PPPoE profile.

The **snmp-server enable traps pppoe** command must be configured in order for SNMP traps to be generated when the PPPoE session-count threshold is reached.

Examples

The following example shows the global PPPoE profile configured with a maximum PPPoE session limit of 8000 sessions. The PPPoE session-count threshold is set at 7000 sessions, so when the number of PPPoE sessions on the router reaches 7000, an SNMP trap will be generated.

```
Router> enable
Router(config)# bba-group pppoe global

Router(config-bba-group)# virtual-template 1

Router(config-bba-group)# sessions max limit 8000 threshold 7000
Router(config-bba-group)# sessions per-vc limit 8
```

```
Router(config-bba-group)# sessions per-mac limit 2
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions permitted over a VC and sets the PPPoE session-count threshold.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions per VLAN in a PPPoE profile.
snmp-server enable traps pppoe	Enables PPPoE session-count SNMP notifications.

sessions per-mac iwf limit

To set the maximum number of Interworking Functionality (IWF) sessions allowed per MAC address in a PPP over Ethernet (PPPoE) profile, use the **sessions per-mac iwf limit**command in BBA group configuration mode. To remove this setting, use the **no** form of this command.

sessions per-mac iwf limit *per-mac-limit*
no sessions per-mac iwf limit *per-mac-limit*

Syntax Description

| *per-mac-limit* | Maximum number of PPPoE sessions that can be sourced from a MAC address. |

Command Default

The normal MAC address session limit (default is 100 sessions) is applied to IWF sessions.

Command Modes

BBA group configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **sessions per-mac iwf limit**command to configure a PPPoE profile with the maximum number of IWF-specific sessions allowed per MAC address.

You cannot configure PPPoE session limits in PPPoE profiles and in virtual private dialup network (VPDN) groups simultaneously. You also cannot configure session limits in PPPoE profiles and directly on PPPoE ports (Ethernet interface, VLAN, or permanent virtual circuit [PVC]) simultaneously.

Examples

The following example shows a limit of two PPPoE sessions per MAC address configured in the global PPPoE profile:

```
bba-group pppoe global
 virtual-template 1
 sessions max limit 8000 threshold-sessions 7000
 sessions per-vc limit 8
 sessions per-mac iwf limit 2
```

Related Commands

Command	Description
bba-group pppoe	Enters BBA group configuration mode and creates a PPPoE profile.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile and sets the PPPoE session-count threshold.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions per VLAN in a PPPoE profile.

sessions per-mac limit

To set the maximum number of PPP over Ethernet (PPPoE) sessions allowed per MAC address in a PPPoE profile, use the **sessions per-mac limit**command in BBA group configuration mode. To remove this setting, use the **no** form of this command.

sessions per-mac limit *per-mac-limit*
no sessions per-mac limit

Syntax Description

per-mac-limit	Maximum number of PPPoE sessions that can be sourced from a MAC address. The default is 100 sessions.

Command Default   The default limit is 100 sessions per-MAC.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Aggregation Service Routers.

Usage Guidelines   Use the **sessions per-mac limit**command to set the maximum number of PPP over Ethernet (PPPoE) sessions allowed per MAC address in a PPPoE profile.

You cannot configure PPPoE session limits in PPPoE profiles simultaneously. You also cannot configure the PPPoE profiles directly on PPPoE ports (Ethernet interface, VLAN, or permanent virtual circuit (PVC)) simultaneously.

Examples   The following example shows a limit of two PPPoE sessions per MAC address configured in the global PPPoE profile:

```
bba-group pppoe global
 virtual-template 1
sessions per-mac limit 2
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold.

Command	Description
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile and sets the PPPoE session-count threshold.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions per VLAN in a PPPoE profile.

sessions per-vc limit

To set the maximum number of PPP over Ethernet (PPPoE) sessions to be established over a virtual circuit (VC) in a PPPoE profile and to set the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated, use the **sessions per-vc limit** command in BBA group configuration mode. To remove this specification, use the **no** form of this command.

sessions per-vc limit *per-vc-limit* [**threshold** *threshold-value*]
no sessions per-vc limit

Syntax Description

per-vc-limit	Maximum number of PPPoE sessions that can be established over an ATM PVC. The default is 100 sessions.
threshold	(Optional) Sets the PPPoE session-count threshold at which an SNMP trap is generated.
threshold-value	(Optional) Number of PPPoE sessions that causes an SNMP trap to be generated.

Command Default

The default limit is 100 sessions per-VC.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Service Routers.

Usage Guidelines

Use the **sessions per-vc limit** command to configure a PPPoE profile with the maximum number of PPPoE sessions that will be allowed per VC.

You cannot configure session limits in PPPoE profiles and directly on permanent virtual circuits (PVCs) simultaneously.

The **snmp-server enable traps pppoe** command must be configured in order for SNMP traps to be generated when the PPPoE session-count threshold is reached.

Examples

The following example shows a limit of eight PPPoE sessions per VC configured in the PPPoE profile "vpn1":

```
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 600 threshold 400
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions per VLAN in a PPPoE profile.
snmp-server enable traps pppoe	Enables PPPoE session-count SNMP notifications.

sessions per-vlan limit

To specify the maximum number of PPP over Ethernet (PPPoE) sessions permitted per VLAN in a PPPoE profile, use the **sessions per-vlan limit**command in BBA group configuration mode. To remove this specification, use the **no** form of this command.

sessions per-vlan limit *per-vlan-limit* **inner** *inner-vlan-limit*
no sessions per-vlan limit *per-vlan-limit*

Syntax Description

per-vlan-limit	Maximum number of PPPoE sessions permitted under each VLAN, the permitted range between 1 and 65535.
inner	The inner session limit per QinQ inner Vlan-id.
inner-vlan-limit	Maximum inner sessions per QinQ inner Vlan-id, the permitted range between 1 and 65535.

Command Default

The default number of sessions per QinQ inner Vlan-id is 100.

Command Modes

BBA group configuration (config-bba-group)#

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated.
12.2(28)SB	This command was integrated.
Cisco IOS XE 2.3.0	This command was integrated. This command is supported on ASR 1000 series.

Usage Guidelines

Use the **sessions per-vlan limit**command to configure a PPPoE profile with the maximum number of PPPoE sessions that will be allowed per VLAN.

You cannot configure session limits in PPPoE profiles and directly on VLANs simultaneously.

Examples

The following example shows a limit of 200 PPPoE sessions per VLAN configured in the PPPoE profile "vpn1":

```
Router(config)# bba-group pppoe vpn1
Router(config-bba-group)# virtual-template 1
Router(config-bba-group)# sessions per-vlan limit 200 inner 100
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.

Command	Description
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile and sets the PPPoE session-count threshold.

sessions pre-auth limit ignore

To enable the local session limit configured on the BRAS or LAC to override the per-NAS-port session limit downloaded from the RADIUS server when Subscriber Service Switch (SSS) preauthorization is configured, use the sessions pre-auth limit ignore command in BBA group configuration mode. To disable the function, use the no form of this command.

sessions pre-auth limit ignore
no sessions pre-auth limit ignore

Syntax Description   This command has no arguments or keywords.

Command Default   The session limit downloaded from RADIUS takes precedence over the local limit.

Command Modes

BBA group configuration mode

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	Ths command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines   The sessions pre-auth limit ignore command is used to enable the PPPoE Session Limit Local Override feature. This feature is useful only when you have configured SSS preauthorization on the BRAS or LAC. If preauthorization is not enabled, the sessions pre-auth limit ignore command has no effect.

When the subscriber access pppoe pre-authorize nas-port-id command is enabled (that is, SSS preauthorization on the LAC is enabled), the PPPoE per-NAS-port session limit downloaded from the RADIUS customer profile database overrides any session limit per VC and per VLAN that you have configured locally.

When the sessions pre-auth limit ignore command is used and SSS preauthorization is configured, the LAC handles the session limit checking as if the subscriber access pppoe pre-authorize nas-port-id command were disabled; that is, the locally configured per-VC or per-VLAN session limit is applied instead of downloading the PPPoE per-NAS-port session limits that are maintained in the RADIUS server.

If you specify the sessions pre-auth limit ignore command and enable preauthorization, but there are no locally configured per-port session limits, then per-NAS-port session limits downloaded from RADIUS are applied.

Examples   The following example enables the local session limit configured on the LAC to override the per-NAS-port session limit configured on the RADIUS server for the PPPoE profile "vpn1":

```
Router(config)# bba-group pppoe vpn1
Router(config-bba-group)# sessions pre-auth limit ignore
```

The following example re-enables the standard functionality of the the subscriber access pppoe pre-authorize nas-port-id command for the PPPoE profile "vpn1":

```
Router(config)# bba-group pppoe vpn1
Router(config-bba-group)# no sessions pre-auth limit ignore
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
subscriber access ppoe pre-authorize nas-port-id	Configures a NAS to enable SSS to preauthorize the NAS port identifier (NAS-Port-ID) string before authorizing the domain name.

sessions per-vlan throttle

To control and throttle the number of PPP over Ethernet (PPPoE) session establishment attempts per MAC address in a particular VLAN, use the **sessions per-vlan throttle** command in BBA group configuration mode. To disable this configuration, use the **no** form of this command.

sessions per-vlan throttle *number-of-sessions session-length session-delay*
no sessions per-vlan throttle *number-of-sessions session-length session-delay*

Syntax Description

number-of-sessions	Maximum number of discovery attempts per VLAN for a given MAC address.
session-length	Permitted time in seconds for the maximum number of sessions per VLAN.
session-delay	The time in seconds that further PPPoE session establishment attempts are blocked from the MAC address.

Command Default　No configuration to throttle the PPPoE sessions per VLAN.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(33)SB	This command was introduced.
Cisco IOS XE Release 2.4.0	This command was integrated. The **throttle** keyword was added.

Usage Guidelines　This command is used to throttle PPPoE discovery attempts in an aggregation deployment when multiple CPEs share the same MAC address, in different VLANs. It allows a per-VLAN throttling mechanism on a per-MAC address basis. The **sessions per-mac throttle** command works in a Broadband Aggregation System (BRAS) global scenario, since the same MAC address is seen in different VLANs.

If the value specified in the *number-of-sessions* argument, in a time-interval defined by the *session-length* argument is exceeded on a particular VLAN, then the particular MAC address is throttled for the period specified in the *session-delay* argument.

Examples　In the following example, a maximum of 100 sessions can be established on each MAC address on each VLAN, in 5 seconds, with a 5-second delay, before a new session request is allowed. The 101st session request causes a 5-second delay before a new session request is allowed:

```
Router(config)# bba-group pppoe global
Router(config-bba-group)# sessions per-vlan
 throttle 100 5 5
```

Related Commands

Command	Description
sessions per-mac throttle	Limits the number of PPPoE session requests that can be made from a single MAC address.

Command	Description
sessions per-vc throttle	Limits the number of PPPoE session requests that can be made from a single VC.

session retry limit

To set the session retry count. Whenever a TR-069 Agent session establishment fails with the auto-configuration server (ACS), the session will be retried for a specified number of times. Use the **session retry limit** command in TR-069 Agent configuration mode.

session retry limit *session-count*

Syntax Description

session-count	The number of retry count sessions. The range for the session count is 0 to 15. The default value is 11.

Command Default The session retry count is set to 11.

Command Modes

TR-069 Agent configuration mode (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples The following example shows how to set the session retry count to 10 whenever a TR-069 Agent session establishment fails with the ACS:

```
Device(config-cwmp)# session retry limit 10
```

sessions throttle

To configure PPP over Ethernet (PPPoE) connection throttling, which limits the number of PPPoE session requests that can be made from a Virtual Circuit (VC) or a Media Access Control (MAC) address within a specified period of time, use the **sessions throttle** command in BBA group configuration mode. To remove this limit, use the **no** form of this command.

sessions {**per-mac** | **per-vc** | **per-vlan**} **throttle** *session-requests session-request-period blocking-period*
no sessions {**per-mac** | **per-vc** | **per-vlan**} **throttle** *session-requests session-request-period blocking-period*

Syntax Description		
per-mac	Limits the number of PPPoE session requests that can be made from a single MAC address.
per-vc	Limits the number of PPPoE session requests that can be made from a single VC.
per-vlan	Limits the number of PPPoE session requests that can be made from a single VLAN.
session-requests	Number of PPPoE session requests that will be allowed within a specified period of time. Range is from 1 to 100000.
session-request-period	Period of time, in seconds, during which a specified number of PPPoE session requests will be allowed. Range is from 1 to 3600.
blocking-period	Period of time, in seconds, during which PPPoE session requests will be blocked. This period begins when the number of PPPoE session requests from a VC, VLAN, or MAC address exceeds the configured *session-requests* value within the configured *session-request-period*. Range is from 0 to 3600.

Command Default The number of PPPoE session requests that can be made within a specific period of time is not limited.

Command Modes

BBA group configuration (config-bba-group)

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. The **per-vlan**keyword was added.

Usage Guidelines Continuous requests to initiate PPPoE sessions can seriously affect the performance of a router and RADIUS server. Use the **sessions throttle** command to configure the PPPoE server to limit the number of requests for PPPoE sessions that can be made from a MAC address or VC during a configured period of time.

If a client exceeds the configured number of allowable session requests (*session-requests*) within the configured time limit (*session-request-period*), the PPPoE server accepts only the allowable number of session requests

and blocks the MAC address or VC from making any more requests for a configured period of time (*blocking-period*).

After the *blocking-period* expires, the PPPoE server will again accept the configured number of session requests from the MAC address or VC within the configured *session-request-period*.

Note All the Interworking Functionality (IWF) sessions may have a similar mac adddress. The **sessions per-mac iwf limit** command enables you to define how many sessions can be terminated per mac with an IWF tag set.

Note The **sessions per-mac throttle** command is applicable to both IWF and non-IWF sessions. Throttling per mac on IWF sessions can seriously affect the call setup for such sessions as each IWF session may use the same MAC address. Therefore it is not recommended to throttle the IWF sessions.

Examples

The following example shows the configuration of per-MAC, per-VC, and per-VLAN PPPoE connection throttling in PPPoE profile "grp1":

```
bba-group pppoe grp1
 virtual-template 1
 sessions per-mac throttle 10 60 300
 sessions per-vc throttle 100 30 300
 sessions per-vlan throttle 50 60 300
interface ATM2/0.1 multipoint
 pvc 2/100
  encapsulation aal5snap
  protocol pppoe group grp1
interface virtual-template1
 ip address negotiated
 no peer default ip address
 ppp authentication chap
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile and sets the PPPoE session-count threshold.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions to be established over a VLAN in a PPPoE profile and sets the PPPoE session-count threshold.