Subcriber Service Switch

The Subscriber Service Switch feature directs PPP between points using a Layer 2 subscriber policy. It also provides the following features for Internet service provides (ISPs):

- Flexible connection options for subscribers seeking available services
- Flexible number of subscribers
- Flexible definition of services

Configuration Information

Configuration information is included in the "How to Configure a Subscriber Service Switch Policy" module in the "Configuring Cisco Subscriber Service Switch Policies" chapter of the *Cisco IOS Broadband and DSL Configuration Guide,* Release 12.4.

Command Reference Information

This section documents modified commands.

- **atm pppatm passive**
- **clear pppatm interface atm**
- **clear pppoe**
- **debug pppatm**
- **debug sss aaa authorization event**
- **debug sss aaa authorization fsm**
- **debug sss error**
- **debug sss event**
- **debug sss fsm**
- **multihop-hostname**
- **show pppatm summary**
- **show pppatm trace**
- **show sss session**
- **show vpdn session**
- **subscriber access**
- **subscriber authorization enable**
- **vpdn authorize domain**

- **vpn service**

atm pppatm passive

To place an ATM subinterface in passive mode, use the **atm pppatm passive** command in ATM subinterface configuration mode. To change the configuration back to the default (active) mode, use the **no** form of this command.

atm pppatm passive

no atm pppatm passive

Syntax Description

This command has no arguments or keywords.

Defaults

Active mode

Command Modes

ATM subinterface configuration

Command History

Release	Modification
12.2(13)T	This feature was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **atm pppatm passive** command places PPP over ATM (PPPoA) sessions on an ATM subinterface in "listening" mode. Rather than trying to establish the sessions actively by sending out Link Control Protocol (LCP) packets, these sessions listen to the incoming LCP packets and become active only after they have received their first LCP packet. This feature is useful for L2TP access concentrators (LACs) in the broadband access deployments where thousands of PPPoA sessions are configured on LACs. When PPPoA is in the passive mode, the LAC will bring up the sessions only when the subscribers become active and not waste its processing power on polling all the sessions.

For better scalability and faster convergence of PPP sessions, Cisco recommends setting the PPPoA sessions to passive mode at the LAC.

Examples

The following example configures the passive mode for the PPPoA sessions on an ATM subinterface:

```
interface atm 1/0.1 multipoint
 atm pppatm passive
 range range-pppoa-1 pvc 100 199
  protocol ppp virtual-template 1
```

clear pppatm interface atm

To clear PPP ATM sessions on an ATM interface, use the **clear pppatm interface atm** command in privileged EXEC mode.

clear pppatm interface atm *interface-number*[**.***subinterface-number*] [**vc** {[*vpi***/**]*vci* | *virtual-circuit-name*}]

Syntax Description

interface-number	ATM interface number.
.*subinterface-number*	(Optional) ATM subinterface number. A period must precede the number.
vc [*vpi***/**]*vci*	(Optional) Specifies virtual circuit (VC) by virtual path identifier (VPI) and virtual channel identifier (VCI). A slash must follow the VPI.
vc *virtual-circuit-name*	(Optional) Specifies VC by name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command clears the PPP over ATM (PPPoA) sessions in an interface, or in a VC when the VC is specified.

When the **clear pppatm interface atm** command is used to clear sessions on an interface, PPP keepalives continue to work and can be used to detect a broken link.

Examples

The following example clears a PPP ATM session on ATM interface 1/0.10:

```
Router# clear pppatm interface atm 1/0.10
```

Related Commands

Command	Description
debug pppatm	Enables reports for PPPoA events, errors, and states either globally or conditionally on an interface or VC.
show pppatm summary	Displays PPPoA session counts.

clear pppoe

To clear PPP over Ethernet (PPPoE) sessions, use the **clear pppoe** command in privileged EXEC mode.

clear pppoe {**interface** *type number* [**vc** {[*vpi*/]*vci* | *vc-name*}] [**vlan** *vlan-id*] | **rmac** *mac-address* [**sid** *session-id*] | **all**}

Syntax Description

interface *type number*	Interface keyword followed by the interface type and number.
vc [*vpi*/]*vci*	(Optional) Virtual circuit (VC) keyword followed by a virtual path identifier (VPI), virtual channel identifier (VCI). A slash (/) follows the VPI.
vc *vc-name*	(Optional) Name of the VC.
vlan *vlan-id*	(Optional) VLAN identifier.
rmac *mac-address*	(Optional) Remote MAC address.
sid *session-id*	(Optional) Session identifier.
all	(Optional) Specifies that all PPPoE sessions will be cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(2)T	The **vlan** *vlan-id* keyword and argument were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **clear pppoe all** command to clear all PPPoE sessions.

Use the **interface** keyword and arguments and the **vlan** keyword and argument to clear PPPoE sessions on a specific Ethernet 802.1Q VLAN.

Use the **interface**, **vc**, and **vlan** keywords and arguments to clear PPPoE over 802.1Q VLAN sessions on an ATM PVC.

Examples

The following example clears all PPPoE sessions:

```
Router# clear pppoe all
```

debug pppatm

To enable debug reports for PPP over ATM (PPPoA) events, errors, and states, either globally or conditionally, on an interface or virtual circuit (VC), use the **debug pppatm** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug pppatm {**event** | **error** | **state**} [**interface atm** *interface-number* [*subinterface-number*]] **vc** {[*vpi/vci*]*vci* | *virtual-circuit-name*}

no debug pppatm {**event** | **error** | **state**} [**interface atm** *interface-number* [*subinterface-number*] **vc** {[*vpi/*]*vci* | *virtual-circuit-name*}

Syntax Description

event	PPPoA events.
error	PPPoA errors.
state	PPPoA state.
interface atm *interface-number* [*subinterface-number*]	(Optional) Specifies a particular ATM interface by interface number and optionally a subinterface number separated by a period.
vc [*vpi/*]*vci virtual-circuit-name*	(Optional) Virtual circuit (VC) keyword followed by a virtual path identifier (VPI), virtual channel identifier (VCI), and VC name. A slash mark is required after the VPI.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Each specific PPPoA debug report must be requested on a separate command line; see the "Examples" section.

Examples

The following is example output of a PPPoA session with event, error, and state debug reports enabled on ATM interface 1/0.10:

```
Router# debug pppatm event interface atm1/0.10
Router# debug pppatm error interface atm1/0.10
Router# debug pppatm state interface atm1/0.10

00:03:08: PPPATM: ATM1/0.10 0/101 [1], Event = Clear Session
00:03:08: PPPATM: ATM1/0.10 0/101 [1], Event = Disconnecting
00:03:08: PPPATM: ATM1/0.10 0/101 [1], Event = AAA gets dynamic attrs
00:03:08: PPPATM: ATM1/0.10 0/101 [1], Event = AAA gets dynamic attrs
```

```
00:03:08: PPPATM: ATM1/0.10 0/101 [1], Event = SSS Cleanup
00:03:08: PPPATM: ATM1/0.10 0/101 [0], State = DOWN
00:03:08: PPPATM: ATM1/0.10 0/101 [0], Event = Up Pending
00:03:16: PPPATM: ATM1/0.10 0/101 [0], Event = Up Dequeued
00:03:16: PPPATM: ATM1/0.10 0/101 [0], Event = Processing Up
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = Access IE allocated
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = Set Pkts to SSS
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = AAA gets retrived attrs
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = AAA gets nas port details
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = AAA gets dynamic attrs
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = AAA gets dynamic attrs
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = AAA unique id allocated
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = No AAA method list set
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = SSS Request
00:03:16: PPPATM: ATM1/0.10 0/101 [2], State = NAS_PORT_POLICY_INQUIRY
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = SSS Msg Received = 1
00:03:16: PPPATM: ATM1/0.10 0/101 [2], State = PPP_START
00:03:16: PPPATM: ATM1/0.10 0/101 [2], Event = PPP Msg Received = 1
00:03:16: PPPATM: ATM1/0.10 0/101 [2], State = LCP_NEGOTIATION
00:03:27: PPPATM: ATM1/0.10 0/101 [2], Event = PPP Msg Received = 4
00:03:27: PPPATM: ATM1/0.10 0/101 [2], Event = HW Switch support FORW = 0
00:03:27: PPPATM: ATM1/0.10 0/101 [2], Event = Access IE get nas port
00:03:27: PPPATM: ATM1/0.10 0/101 [2], Event = AAA gets dynamic attrs
00:03:27: PPPATM: ATM1/0.10 0/101 [2], Event = AAA gets dynamic attrs
00:03:27: PPPATM: ATM1/0.10 0/101 [2], Event = PPP Msg Received = 5
00:03:27: PPPATM: ATM1/0.10 0/101 [2], Event = Set Pkts to SSS
00:03:27: PPPATM: ATM1/0.10 0/101 [2], State = FORWARDED
```

Table 1 describes the significant fields shown in the display.

Table 1 debug pppatm Field Descriptions

Field	Description
Event	Reports PPPoA events for use by Cisco engineering technical assistance personnel.
State	Reports PPPoA states for use by Cisco engineering technical assistance personnel.

Related Commands

Command	Description
atm pppatm passive	Places an ATM subinterface into passive mode.
show pppatm summary	Displays PPPoA session counts.

debug sss aaa authorization event

To display messages about authentication, authorization, and accounting (AAA) authorization events that are part of normal call establishment, use the **debug sss aaa authorization event** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug sss aaa authorization event

no debug sss aaa authorization event

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following is sample output of several Subscriber Service Switch (SSS) **debug** commands including the **debug sss aaa authorization event** command. The reports from these commands should be sent to technical personnel at Cisco Systems for evaluation.

```
Router# debug sss event
Router# debug sss error
Router# debug sss state
Router# debug sss aaa authorization event
Router# debug sss aaa authorization fsm

SSS:
  SSS events debugging is on
  SSS error debugging is on
  SSS fsm debugging is on
  SSS AAA authorization event debugging is on
  SSS AAA authorization FSM debugging is on

*Mar  4 21:33:18.248: SSS INFO: Element type is Access-Type, long value is 3
*Mar  4 21:33:18.248: SSS INFO: Element type is Switch-Id, long value is -1509949436
*Mar  4 21:33:18.248: SSS INFO: Element type is Nasport, ptr value is 6396882C
*Mar  4 21:33:18.248: SSS INFO: Element type is AAA-Id, long value is 7
*Mar  4 21:33:18.248: SSS INFO: Element type is AAA-ACCT_ENBL, long value is 1
*Mar  4 21:33:18.248: SSS INFO: Element type is AccIe-Hdl, ptr value is 78000006
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Event service-request, state changed from
wait-for-req to wait-for-auth
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Handling Policy Authorize (1 pending sessions)
*Mar  4 21:33:18.248: SSS PM [uid:7]: Need the following key: Unauth-User
*Mar  4 21:33:18.248: SSS PM [uid:7]: Received Service Request
```

```
*Mar  4 21:33:18.248: SSS PM [uid:7]: Event <need keys>, State: initial-req to
need-init-keys
*Mar  4 21:33:18.248: SSS PM [uid:7]: Policy reply - Need more keys
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Got reply Need-More-Keys from PM
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Event policy-or-mgr-more-keys, state changed from
wait-for-auth to wait-for-req
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Handling More-Keys event
*Mar  4 21:33:20.256: SSS INFO: Element type is Unauth-User, string value is
nobody2@xyz.com
*Mar  4 21:33:20.256: SSS INFO: Element type is AccIe-Hdl, ptr value is 78000006
*Mar  4 21:33:20.256: SSS INFO: Element type is AAA-Id, long value is 7
*Mar  4 21:33:20.256: SSS INFO: Element type is Access-Type, long value is 0
*Mar  4 21:33:20.256: SSS MGR [uid:7]: Event service-request, state changed from
wait-for-req to wait-for-auth
*Mar  4 21:33:20.256: SSS MGR [uid:7]: Handling Policy Authorize (1 pending sessions)
*Mar  4 21:33:20.256: SSS PM [uid:7]: Received More Initial Keys
*Mar  4 21:33:20.256: SSS PM [uid:7]: Event <rcvd keys>, State: need-init-keys to
check-auth-needed
*Mar  4 21:33:20.256: SSS PM [uid:7]: Handling Authorization Check
*Mar  4 21:33:20.256: SSS PM [uid:7]: Event <send auth>, State: check-auth-needed to
authorizing
*Mar  4 21:33:20.256: SSS PM [uid:7]: Handling AAA service Authorization
*Mar  4 21:33:20.256: SSS PM [uid:7]: Sending authorization request for 'xyz.com'
*Mar  4 21:33:20.256: SSS AAA AUTHOR [uid:7]:Event <make request>, state changed from idle
to authorizing
*Mar  4 21:33:20.256: SSS AAA AUTHOR [uid:7]:Authorizing key xyz.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:AAA request sent for key xyz.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Received an AAA pass
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Event <found service>, state changed from
authorizing to complete
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Found service info for key xyz.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Event <free request>, state changed from
complete to terminal
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Free request
*Mar  4 21:33:20.264: SSS PM [uid:7]: Event <found>, State: authorizing to end
*Mar  4 21:33:20.264: SSS PM [uid:7]: Handling Service Direction
*Mar  4 21:33:20.264: SSS PM [uid:7]: Policy reply - Forwarding
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Got reply Forwarding from PM
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Event policy-start-service-fsp, state changed from
wait-for-auth to wait-for-service
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Handling Connect-Forwarding-Service event
*Mar  4 21:33:20.272: SSS MGR [uid:7]: Event service-fsp-connected, state changed from
wait-for-service to connected
*Mar  4 21:33:20.272: SSS MGR [uid:7]: Handling Forwarding-Service-Connected event
```

Related Commands

Command	Description
debug sss aaa authorization fsm	Displays information about AAA authorization state changes.
debug sss error	Displays diagnostic information about errors that may occur during Subscriber Service Switch call setup.
debug sss event	Displays diagnostic information about Subscriber Service Switch call setup events.
debug sss fsm	Displays diagnostic information about the Subscriber Service Switch call setup state.

debug sss aaa authorization fsm

To display information about authentication, authorization, and accounting (AAA) authorization state changes, use the **debug sss aaa authorization fsm** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug sss aaa authorization fsm

no debug sss aaa authorization fsm

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following example shows how to enter this command. See the "Examples" section of the **debug sss aaa authorization event** command page for an example of output.

```
Router# debug sss aaa authorization fsm
```

Related Commands

Command	Description
debug sss aaa authorization event	Displays messages about AAA authorization events that are part of normal call establishment.
debug sss error	Displays diagnostic information about errors that may occur during Subscriber Service Switch call setup.
debug sss event	Displays diagnostic information about Subscriber Service Switch call setup events.
debug sss fsm	Displays diagnostic information about the Subscriber Service Switch call setup state.

debug sss error

To display diagnostic information about errors that may occur during Subscriber Service Switch (SSS) call setup, use the **debug sss error** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug sss error

no debug sss error

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following example shows how to enter this command. See the "Examples" section of the **debug sss aaa authorization event** command page for an example of output.

```
Router# debug sss error
```

Related Commands

Command	Description
debug sss aaa authorization event	Displays messages about AAA authorization events that are part of normal call establishment.
debug sss aaa authorization fsm	Displays information about AAA authorization state changes.
debug sss event	Displays diagnostic information about Subscriber Service Switch call setup events.
debug sss fsm	Displays diagnostic information about the Subscriber Service Switch call setup state.

debug sss event

To display diagnostic information about Subscriber Service Switch (SSS) call setup events, use the **debug sss event** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug sss event

no debug sss event

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following example shows how to enter this command. See the "Examples" section of the **debug sss aaa authorization event**command page for an example of output.

```
Router# debug sss event
```

Related Commands

Command	Description
debug sss aaa authorization event	Displays messages about AAA authorization events that are part of normal call establishment.
debug sss aaa authorization fsm	Displays information about AAA authorization state changes.
debug sss error	Displays diagnostic information about errors that may occur during Subscriber Service Switch call setup.
debug sss fsm	Displays diagnostic information about the Subscriber Service Switch call setup state.

debug sss fsm

To display diagnostic information about the Subscriber Service Switch (SSS) call setup state, use the **debug sss fsm** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug sss fsm

no debug sss fsm

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following example shows how to enter this command. See the "Examples" section of the **debug sss aaa authorization event** command page for an example of output.

```
Router# debug sss fsm
```

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

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 will remove the **multihop-hostname** configuration.

Examples

The following example configures a Layer 2 Tunnel 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.
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.

show pppatm summary

To display PPP over ATM (PPPoA) session counts, use the **show pppatm summary** command in privileged EXEC mode.

show pppatm summary [**interface atm** *interface-number*[**.***subinterface-number*]]

Syntax Description

interface atm *interface-number***.***subinterface-number*	(Optional) Specifies a particular ATM interface by interface number and possibly a subinterface number. A period (**.**) must precede the optional subinterface number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command is useful for obtaining session counts, the state of the PPPoA sessions, and the interfaces on which they are running.

This command gives a summary of the number of PPPoA sessions in each state and the session information of each individual session. If a subinterface number is given in the command, the output is a summary report of the PPPoA sessions in the subinterface. If a main interface number is given, the output will have the summary reports for each individual subinterface of that main interface as shown in the Examples section. If no interface is given, the output will contain the summary reports for each ATM interface on the router.

Examples

The following example displays PPPoA session counts and states for ATM interface 5/0:

```
Router# show pppatm summary interface atm 5/0

ATM5/0.3:

       0 sessions total

ATM5/0.6:
       1 in PTA (PTA) State

       1 sessions total

VPI     VCI     Conn ID         PPPoA ID        SSS ID          PPP ID        AAA ID   VT
VA/SID  State
  6     101       11           DA000009       BB000013       E5000017        C        1
1.1     PTA
```

Most of the fields displayed by the **show pppatm summary** command are self-explanatory. Table 2 describes the significant fields shown in the displays. Any data not described in Table 2 is used for internal debugging purposes.

Table 2 show pppatm summary Field Descriptions

Field	Description
VPI	Virtual path identifier of the permanent virtual circuit (PVC).
VCI	Virtual channel identifier of the PVC.
Conn ID	Unique connection identifier for the PPPoA session. This ID can be correlated with the unique ID in the **show vpdn session** command output for the forwarded sessions.
PPPoA ID	Internal identifier for the PPPoA session.
SSS ID	Internal identifier in the Subscriber Service Switch.
PPP ID	Internal identifier in PPP.
AAA ID	Authentication, authorization, and accounting (AAA) unique identifier for accounting records.
VT	Virtual template number used by the session.
VA/SID	PPPoA virtual access number for PPP Termination Aggregation (PTA) sessions, and switch identifier for forwarded sessions.
State	PPPoA state of the session.

Related Commands

Command	Description
clear pppatm interface atm	Clears PPP ATM sessions on an ATM interface.
debug pppatm	Enables reports for PPPoA events, errors, and states either globally or conditionally on an interface or VC.
show pppatm trace	Displays a sequence of PPPoA events, errors, and state changes when the **debug pppatm** command is enabled.

show pppatm trace

To display a sequence of PPP over ATM (PPPoA) events, errors, and state changes when the **debug pppatm** command is enabled, use the **show pppatm trace** command in privileged EXEC mode.

show pppatm trace [**error** | **event** | **state**] **interface atm** *interface-number*[**.***subinterface-number*] **vc** {[*vpi***/**]*vci* | *virtual-circuit-name*}

Syntax Description

error	(Optional) PPPoA events.
event	(Optional) PPPoA errors.
state	(Optional) PPPoA state.
interface atm *interface-number*	Specifies a particular ATM interface by interface number.
.*subinterface-number*	(Optional) Specifies a subinterface number preceded by a period.
vc [*vpi***/**]*vci*	Virtual circuit (VC) keyword followed by a virtual path identifier (VPI) and virtual channel identifier (VCI). The absence of the "**/**" and a *vpi* causes the *vpi* value to default to 0.
virtual-circuit-name	Name of the VC.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

When the **debug pppatm** command has been enabled, this command displays messages from the specified permanent virtual circuit (PVC). If only one **debug pppatm** command keyword is supplied in the command, the report will display only the sequence of events for that particular debug type.

Examples

The following example traces the debugging messages supplied by the **debug pppatm** command on PVC 101. The report is used by Cisco technical personnel for diagnosing system problems.

```
Router# debug pppatm trace interface atm 1/0.10 vc 101
Router# debug pppatm state interface atm 1/0.10 vc 101
Router# debug pppatm event interface atm 1/0.10 vc 101
Router# show pppatm trace interface atm 1/0.10 vc 101

Event = Disconnecting
Event = AAA gets dynamic attrs
Event = AAA gets dynamic attrs
Event = SSS Cleanup
State = DOWN
Event = Up Pending
Event = Up Dequeued
Event = Processing Up
```

```
Event = Access IE allocated
Event = Set Pkts to SSS
Event = AAA gets retrieved attrs
Event = AAA gets nas port details
Event = AAA gets dynamic attrs
Event = AAA gets dynamic attrs
Event = AAA unique id allocated
Event = No AAA method list set
Event = SSS Request
State = NAS_PORT_POLICY_INQUIRY
Event = SSS Msg
State = PPP_START
Event = PPP Msg
State = LCP_NEGOTIATION
Event = PPP Msg
Event = Access IE get nas port
Event = AAA gets dynamic attrs
Event = AAA gets dynamic attrs
Event = PPP Msg
Event = Set Pkts to SSS
State = FORWARDED
```

Related Commands

Command	Description
clear pppatm interface atm	Clears PPP ATM sessions on an ATM interface.
debug pppatm	Enables reports for PPPoA events, errors, and states either globally or conditionally on an interface or VC.
show pppatm summary	Displays PPPoA session counts.

show sss session

To display Subscriber Service Switch session status, use the **show sss session** command in privileged EXEC mode.

show sss session [**all**]

Syntax Description

all	(Optional) Provides an extensive report about the Subscriber Service Switch sessions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to verify correct operation of PPP connections in the Subscriber Service Switch environment.

Examples

The following sample output from the **show sss session** command provides a basic report of Subscriber Service Switch session activity:

```
Router# show sss session

Current SSS Information: Total sessions 9

Uniq ID Type       State         Service      Identifier           Last Chg
9       PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:02:36
10      PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:01:52
11      PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:01:52
3       PPPoE/PPP  connected     VPDN         user3@cisco.com          2d21h
6       PPPoE/PPP  connected     Local Term   user1                    00:03:35
7       PPPoE/PPP  connected     Local Term   user2                    00:03:35
8       PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:02:36
2       PPP        connected     Local Term   user5                    00:05:06
4       PPP        connected     VPDN         nobody2@cisco.com        00:06:52
```

The following sample output from the **show sss session all** command provides a more extensive report of Subscriber Service Switch session activity:

```
Router# show sss session all

Current SSS Information: Total sessions 9

SSS session handle is 40000013, state is connected, service is VPDN
Unique ID is 9
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:49
```

```
Root SIP Handle is DF000010, PID is 49
AAA unique ID is 10
Current SIP options are Req Fwding/Req Fwded

SSS session handle is B0000017, state is connected, service is VPDN
Unique ID is 10
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:05
Root SIP Handle is B9000015, PID is 49
AAA unique ID is 11
Current SIP options are Req Fwding/Req Fwded

SSS session handle is D6000019, state is connected, service is VPDN
Unique ID is 11
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:13
Root SIP Handle is D0000016, PID is 49
AAA unique ID is 12
Current SIP options are Req Fwding/Req Fwded

SSS session handle is 8C000003, state is connected, service is VPDN
Unique ID is 3
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user3@cisco.com
Last Changed 2d21h
Root SIP Handle is D3000002, PID is 49
AAA unique ID is 3
Current SIP options are Req Fwding/Req Fwded

SSS session handle is BE00000B, state is connected, service is Local Term
Unique ID is 6
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user1
Last Changed 00:03:56
Root SIP Handle is A9000009, PID is 49
AAA unique ID is 7
Current SIP options are Req Fwding/Req Fwded

SSS session handle is DC00000D, state is connected, service is Local Term
Unique ID is 7
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user2
Last Changed 00:03:57
Root SIP Handle is 2C00000A, PID is 49
AAA unique ID is 8
Current SIP options are Req Fwding/Req Fwded

SSS session handle is DB000011, state is connected, service is VPDN
Unique ID is 8
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:58
Root SIP Handle is 1000000F, PID is 49
AAA unique ID is 9
Current SIP options are Req Fwding/Req Fwded

SSS session handle is 3F000007, state is connected, service is Local Term
Unique ID is 2
SIP subscriber access type(s) are PPP
Identifier is user5
Last Changed 00:05:30
Root SIP Handle is 8A000009, PID is 92
```

```
AAA unique ID is 1
Current SIP options are Req Fwding/Req Fwded

SSS session handle is 97000005, state is connected, service is VPDN
Unique ID is 4
SIP subscriber access type(s) are PPP
Identifier is nobody2@cisco.com
Last Changed 00:07:16
Root SIP Handle is 32000000, PID is 92
AAA unique ID is 5
Current SIP options are Req Fwding/Req Fwded
```

Most of the fields displayed by the **show sss session** and **show sss session all** commands are self-explanatory. Table 3 describes the significant fields shown in the displays. Any data not described in Table 3 is used for internal debugging purposes.

Table 3 show sss session Field Descriptions

Field	Description
Uniq ID	The unique identifier used to correlate this particular session with the sessions retrieved from other **show** commands or **debug** command traces.
Type	Access protocols relevant to this session.
State	Status of the connection, which can be one of the following states: • connected—The session has been established. • wait-for-req—Waiting for request. • wait-for-auth—Waiting for authorization. • wait-for-fwd—Waiting to be forwarded; for example, waiting for virtual private dialup network (VPDN) service.
Service	Type of service given to the user.
Identifier	A string identifying the user. This identifier may either be the username, or the name used to authorize the session.
Last Chg	Time interval in in hh:mm:ss since the service for this session was last changed.

Related Commands

Command	Description
show vpdn session	Displays session information about the L2TP and L2F protocols, and PPPoE tunnels in a VPDN.

show vpdn session

To display session information about active Layer 2 sessions for a virtual private dialup network (VPDN), use the **show vpdn session** command in privileged EXEC mode.

show vpdn session [**l2f** | **l2tp** | **pptp**] [**all** | **packets** | **sequence** | **state** [*filter*]]

Syntax Description

l2f	(Optional) Displays information about Layer 2 Forwarding (L2F) calls only.
l2tp	(Optional) Displays information about Layer 2 Tunnel Protocol (L2TP) calls only.
pptp	(Optional) Displays information about Point-to-Point Tunnel Protocol (PPTP) calls only.
all	(Optional) Displays extensive reports about active sessions.
filter	(Optional) One of the filter parameters defined in Table 4.
packets	(Optional) Displays information about packet and byte counts for sessions.
sequence	(Optional) Displays sequence information for sessions.
state	(Optional) Displays state information for sessions.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	This command was enhanced to display Point-to-Point Protocol over Ethernet (PPPoE) session information. Support was added for the **packets** and **all** keywords.
12.1(2)T	This command was enhanced to display PPPoE session information on actual Ethernet interfaces.
12.2(13)T	Reports from this command were enhanced with a unique identifier that can be used to correlate a particular session with the session information retrieved from other **show** commands or **debug** command traces.
12.3(2)T	Support was added for the **l2f**, **l2tp**, and **pptp** keywords.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **show vpdn session** command to display information about all active sessions using L2TP, L2F, and PPTP.

The output of the **show vpdn session** command displays PPPoE session information as well. PPPoE is supported on ATM permanent virtual connections (PVCs) compliant with RFC 1483 only. PPPoE is not supported on Frame Relay and any other LAN interfaces such as FDDI and Token Ring.

Reports and options for this command depend upon the configuration in which it is used. Use the command-line question mark (?) help function to display options available with the **show vpdn session** command.

Table 4 defines the filter parameters available to refine the output of the **show vpdn session** command. You may use any one of the filter parameters in place of the *filter* argument.

Table 4 Filter Parameters for the show vpdn session Command

Syntax	Description
interface serial *number*	Filters the output to display only information for sessions associated with the specified serial interface. • *number*—The serial interface number.
interface virtual-template *number*	Filters the output to display only information for sessions associated with the specified virtual template. • *number*—The virtual template number.
tunnel id *tunnel-id session-id*	Filters the output to display only information for sessions associated with the specified tunnel ID and session ID. • *tunnel-id*—The local tunnel ID. Valid values range from 1 to 65535. • *session-id*—The local session ID. Valid values range from 1 to 65535.
tunnel remote-name *remote-name local-name*	Filters the output to display only information for sessions associated with the tunnel with the specified names. • *remote-name*—The remote tunnel name. • *local-name*—The local tunnel name.
username *username*	Filters the output to display only information for sessions associated with the specified username. • *username*—The username.

Examples

The **show vpdn session** command provides reports on call activity for all active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session

L2TP Session Information Total tunnels 1 sessions 4

LocID RemID TunID Intf          Username             State    Last Chg Uniq ID
4     691   13695 Se0/0         nobody2@cisco.com        est    00:06:00  4
5     692   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  8
6     693   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  9
3     690   13695 SSS Circuit   nobody3@cisco.com        est    2d21h     3

L2F Session Information Total tunnels 1 sessions 2

 CLID   MID    Username                   Intf          State   Uniq ID
 1      2      nobody@cisco.com              SSS Circuit   open    10
 1      3      nobody@cisco.com              SSS Circuit   open    11

%No active PPTP tunnels

PPPoE Session Information Total tunnels 1 sessions 7

PPPoE Session Information
UID    SID    RemMAC         OIntf          Intf      Session
              LocMAC                        VASt      state
3      1      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
```

```
6       2       0030.949b.b4a0 Fa2/0          Vi1.1     CNCT_PTA
                0010.7b90.0840               UP
7       3       0030.949b.b4a0 Fa2/0          Vi1.2     CNCT_PTA
                0010.7b90.0840               UP
8       4       0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
                0010.7b90.0840
9       5       0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
                0010.7b90.0840
10      6       0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
                0010.7b90.0840
11      7       0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
                0010.7b90.0840
```

Table 5 describes the significant fields in the **show vpdn session** display.

Table 5 show vpdn session Field Descriptions

Field	Description
LocID	Local identifier.
RemID	Remote identifier.
TunID	Tunnel identifier.
Intf	Interface associated with the session.
Username	User domain name.
State	Status for the individual user in the tunnel; can be one of the following states: • est • opening • open • closing • closed • waiting_for_tunnel The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Last Chg	Time interval (in hh:mm:ss) since the last change occurred.
Uniq ID	The unique identifier used to correlate this particular session with the sessions retrieved from other **show** commands or **debug** command traces.
CLID	A number uniquely identifying the session.
MID	A number uniquely identifying this user in this tunnel.
UID	PPPoE user ID.
SID	PPPoE session ID.
RemMAC	Remote MAC address of the host.
LocMAC	Local MAC address of the router. It is the default MAC address of the router.
OIntf	Outgoing interface.

Table 5 show vpdn session Field Descriptions (continued)

Field	Description
Intf VASt	Virtual access interface number and state.
Session state	PPPoE session state.

The **show vpdn session packets** command provides reports on call activity for all the currently active sessions. The following output is from a device carrying an active PPPoE session:

```
Router# show vpdn session packets

%No active L2TP tunnels
%No active L2F tunnels

PPPoE Session Information Total tunnels 1 sessions 1
PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       202333          202337          2832652         2832716
```

Table 6 describes the significant fields shown in the **show vpdn session packets** command display.

Table 6 show vpdn session packets Field Descriptions

Field	Description
SID	Session ID for the PPPoE session.
Pkts-In	Number of packets coming into this session.
Pkts-Out	Number of packets going out of this session.
Bytes-In	Number of bytes coming into this session.
Bytes-Out	Number of bytes going out of this session.

The **show vpdn session all** command provides extensive reports on call activity for all the currently active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session all

L2TP Session Information Total tunnels 1 sessions 4

Session id 5 is up, tunnel id 13695
Call serial number is 3355500002
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:03:53
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface
    Remote session id is 692, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 8

Session id 6 is up, tunnel id 13695
```

```
Call serial number is 3355500003
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:04:22
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface
    Remote session id is 693, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 9

Session id 3 is up, tunnel id 13695
Call serial number is 3355500000
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 2d21h
    48693 Packets sent, 48692 received
    1947720 Bytes sent, 1314568 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody2@cisco.com
    Interface
    Remote session id is 690, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 3

Session id 4 is up, tunnel id 13695
Call serial number is 3355500001
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:08:40
    109 Packets sent, 3 received
    1756 Bytes sent, 54 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface Se0/0
    Remote session id is 691, remote tunnel id 58582
  UDP checksums are disabled
  IDB switching enabled
  FS cached header information:
    encap size = 36 bytes
    4500001C BDDC0000 FF11E977 0A00003E
    0A00003F 06A506A5 00080000 0202E4D6
    02B30000
  Sequencing is off
  Unique ID is 4

L2F Session Information Total tunnels 1 sessions 2
MID: 2
User:  nobody@cisco.com
Interface:
State:  open
Packets out: 53
Bytes out: 2264
```

```
Packets in: 51
Bytes in: 1274
Unique ID: 10

  Last clearing of "show vpdn" counters never
MID: 3
User:  nobody@cisco.com
Interface:
State:  open
Packets out: 53
Bytes out: 2264
Packets in: 51
Bytes in: 1274
Unique ID: 11

Last clearing of "show vpdn" counters never

%No active PPTP tunnels

PPPoE Session Information Total tunnels 1 sessions 7

PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       48696           48696           681765          1314657
2       71              73              1019            1043
3       71              73              1019            1043
4       61              62              879             1567
5       61              62              879             1567
6       55              55              791             1363
7       55              55              795             1363
```

The significant fields shown in the **show vpdn session all** command display are similar to those defined in Table 5 and Table 6.

Related Commands

Command	Description
show sss session	Displays Subscriber Service Switch session status.
show vpdn	Displays basic information about all active VPDN tunnels.
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.

subscriber access

To configure a network access server (NAS) to enable Subscriber Service Switch (SSS) to preauthorize the NAS port identifier (NAS-Port-ID) string before authorizing the domain name, use the **subscriber access** command in global configuration mode. To disable SSS preauthorization, use the **no** form of this command.

subscriber access {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*] [**send username**]

no subscriber access {**pppoe** | **pppoa**} **pre-authorize nas-port-id**

Syntax Description

pppoe	Specifies PPP over Ethernet (PPPoE).
pppoa	Specifies PPP over ATM (PPPoATM).
pre-authorize nas-port-id	Signals SSS to preauthorize the NAS-Port-ID string before authorizing the domain name.
default	(Optional) Uses the default method list name instead of the named *list-name* argument.
list-name	(Optional) Authentication, authorization, and accounting (AAA) authorization configured on the LAC.
send username	(Optional) Specifies to send the authentication username of the session in the Change_Info attribute (attribute 77).

Defaults

Preauthorization is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)B	This command was introduced on the Cisco 6400 series, the Cisco 7200 series, and the Cisco 7401 Application Specific Router (ASR).
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T, and the **pppoe** and **pppoa** keywords were added.
12.4(2)T	The **send username** keyword was added.
12.3(14)YM2	This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7301, Cisco 7204VXR, and Cisco 7206VXR routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The NAS-Port-ID string is used to locate the first service record, which may contain one of three attributes, as follows:

- A restricted set of values for the domain substring of the unauthenticated PPP name.

  This filtered service key then locates the final service. See the **vpdn authorize domain** command for more information.
- PPPoE session limit.
- The logical line ID (LLID).

Once NAS port authorization has taken place, normal authorization, which is usually the domain authorization, continues.

Logical Line ID

The LLID is an alphanumeric string of from 1 to 253 characters that serves as the logical identification of a subscriber line. LLID is maintained in a RADIUS server customer profile database and enables users to track their customers on the basis of the physical lines on which customer calls originate. Downloading the LLID is also referred to as "preauthorization" because it occurs before normal virtual private dialup network (VPDN) authorization downloads L2TP tunnel information.

This command enables LLID and SSS querying only for PPP over Ethernet over ATM (PPPoEoATM) and PPP over Ethernet over VLAN (PPPoEoVLAN or Dot1Q) calls; all other calls, such as ISDN, are not supported.

Per-NAS-Port Session Limits for PPPoE

Use this command to configure SSS preauthorization on the LAC so that the PPPoE per-NAS-port session limit can be downloaded from the customer profile database. To use PPPoE per-NAS-port session limits, you must also configure the PPPoE Session-Limit per NAS-Port Cisco attribute-value pair in the user profile.

Examples

The following example signals SSS to preauthorize the NAS-Port-ID string before authorizing the domain name. This policy applies only to sessions that have a PPPoE access type.

```
aaa new-model
aaa group server radius sg_llid
 server 172.20.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_group
 server 172.20.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg_group
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_group password 0 lab
vpdn enable
!
vpdn-group 2
  request-dialin
  protocol l2tp
 domain example.com
 initiate-to ip 10.1.1.1
 local name s7200_2
!
vpdn-group 3
```

```
 accept dialin
  protocol pppoe
  virtual-template 1
!
! Signals Subscriber Service Switch to preauthorize the NAS-Port-ID string before
! authorizing the domain name.
subscriber access pppoe pre-authorize nas-port-id mlist_llid
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1/0
 ip address 10.2.2.2 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0.1 point-to-point
 pvc 1/100
  encapsulation aa15snap
  protocol pppoe
!
interface virtual-template1
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.20.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.20.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1
```

The following example is identical to the previous example except that it also adds support for sending the PPP authenticating username with the preauthorization in the Connect-Info attribute. This example also includes command-line interface (CLI) suppression on the LLID if the username that is used to authenticate has a domain that includes #184.

```
aaa new-model
aaa group server radius sg_llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_group
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg_group
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_group password 0 lab
vpdn enable
!
vpdn-group 2
 request-dialin
 protocol 12tp
 domain example.com
 domain example.com#184
```

```
 initiate-to ip 10.1.1.1
 local name s7200_2
 l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
 accept dialin
 procotol pppoe
 virtual-template 1
!
subscriber access pppoe pre-authorize nas-port-id mlist_llid send username
!
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
l2tp attribute clid mask-method	Configure a NAS to provide L2TP calling line ID suppression for calls belonging to a VPDN group.
subscriber authorization enable	Enables SSS type authorization.
vpdn authorize domain	Enables domain preauthorization on a NAS.
vpdn l2tp attribute clid mask-method	Configure a NAS to provide L2TP calling line ID suppression globally on the router.

subscriber authorization enable

To enable Subscriber Service Switch type authorization, use the **subscriber authorization enable** command in global configuration mode. To disable the Subscriber Service Switch authorization, use the **no** form of this command.

subscriber authorization enable

no subscriber authorization enable

Syntax Description

This command has no arguments or keywords.

Defaults

Authorization is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This feature was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **subscriber authorization enable** command triggers Subscriber Service Switch type authorization for local termination, even if virtual private dialup network (VPDN) and Stack Group Bidding Protocol (SGBP) are disabled.

Examples

The following example enables Subscriber Service Switch type authorization:

```
subscriber authorization enable
```

Related Commands

Command	Description
subscriber access	Enables Subscriber Service Switch preauthorizationof a NAS port identifier (NAS-Port-ID) string before authorizing the domain name.
vpdn authorize domain	Enables domain preauthorization on a NAS.

vpdn authorize domain

To enable domain preauthorization on a network access server (NAS), use the **vpdn authorize domain** command in global configuration mode. To disable domain preauthorization, use the **no** form of this command.

vpdn authorize domain

no vpdn authorize domain

Syntax Description

This command has no arguments or keywords.

Defaults

Domain preauthorization is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 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

A domain preauthorization RADIUS user profile must also be created. See the "Examples" section and refer to the *Cisco IOS Security Configuration Guide* for information on how to create these profiles.

Examples

Domain Preauthorization Configuration on the LAC Example

The following example shows the configuration necessary for an L2TP access concentrator (LAC) to participate in domain preauthorization:

```
!
aaa new-model
aaa authorization network default local group radius
!
vpdn authorize domain
!
radius-server host 10.9.9.9 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
radius-server key MyKey
radius-server vsa send authentication
!
```

Domain Preauthorization RADIUS User Profile Example

The following example shows a domain preauthorization RADIUS user profile:

```
user = nas-port:10.9.9.9:0/0/0/30.33{
 profile_id = 826
 profile_cycle = 1
```

```
radius=Cisco {
check_items= {
2=cisco
}
reply_attributes= {
9,1="vpdn:vpn-domain-list=net1.com,net2.com"
6=5
}
}
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

vpn service

To configure a static domain name, use the **vpn service** command in ATM VC, ATM VC class or VC class configuration mode or in PVC range configuration mode. To remove a static domain name, use the **no** form of this command.

vpn service *domain-name* [**replace-authen-domain**]

no vpn service *domain-name* [**replace-authen-domain**]

Syntax Description

domain-name	Static domain name.
replace-authen-domain	(Optional) Specifies that when a static name is configured and VPDN preauthentication is configured, the domain name specified for VPN service replaces the domain field in the username for authentication.

Defaults

No default behavior or values

Command Modes

ATM VC configuration
ATM VC class configuration
PVC range configuration

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(7)XI7	The **replace-authen-domain** keyword was added and this command was integrated into Cisco IOS Release 12.2(7)XI7.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **vpn service** command in a permanent virtual circuit (PVC), VC class configuration, or PVC range configuration so that PPP over ATM (PPPoA) or PPP over Ethernet over ATM (PPPoEoA) sessions in those PVCs will be forwarded according to the domain name supplied, without starting PPP.

To replace the VPN service domain name with the domain name from the username during preauthentication, use this command with the **replace-authen-domain** keyword, in conjunction with the **vpdn authen-before-forward** command.

Examples

In the following partial example, VPDN group 1 is selected for PPPoA session forwarding based on the domain name example.com:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain example.com
 initiate-to ip 10.1.1.1 priority 1
```

```
.
.
.
interface ATM1/0.1 multipoint
 pvc 101
  encapsulation aal5mux ppp virtual-Template 1
  vpn service example.net
```

In the following partial example using the **replace-authen-domain** keyword, the domain field is replaced by the domain name during preauthentication:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain example.net
 authen-before-forward
 initiate-to ip 10.1.1.1 priority 1
.
.
.
interface atm 4/0
 ip address 3.0.0.2 255.255.0.0
 pvc 1/20
encapsulation aal5mux ppp virtual-Template 1
  vpn service example.net replace-authen-domain
```

Related Commands

Command	Description
vpdn authen-before-forward	Enables authentication of all dial-in L2TP sessions before the sessions are forwarded to the tunnel server (global preauthentication).