



Subscriber Service Switch

The Subscriber Service Switch provides flexibility on where and how many subscribers are connected to available services and how those services are defined. The primary focus of Subscriber Service Switch is to direct PPP from one point to another using a Layer 2 subscriber policy. The policy will manage tunneling of PPP in a policy-based bridging fashion.

Feature Specifications for the Subscriber Service Switch Feature

Release	Modification
12.2(13)T	This feature was introduced.
12.2(27)SBA	This feature was integrated into Cisco IOS Release 12.2(27)SBA.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Subscriber Service Switch, page 2](#)
- [Information About Subscriber Service Switch, page 2](#)
- [How to Use Subscriber Service Switch, page 5](#)
- [Configuration Examples for Subscriber Service Switch, page 11](#)
- [Additional References, page 26](#)
- [Command Reference, page 28](#)
- [Glossary, page 62](#)



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002, 2005 Cisco Systems, Inc. All rights reserved.

Restrictions for Subscriber Service Switch

Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. Subscriber Service Switch will provide the infrastructure for any protocol to plug into, but the initial focus will be on switching PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA) sessions to a Layer 2 Tunneling Protocol (L2TP) devices such as an L2TP access concentrator (LAC) switch, and switching L2TP sessions to an L2TP tunnel switch.

Information About Subscriber Service Switch

To configure Subscriber Service Switch, you need to understand the following concepts:

- [Benefits of Subscriber Service Switch, page 2](#)
- [Backward Compatibility, page 3](#)

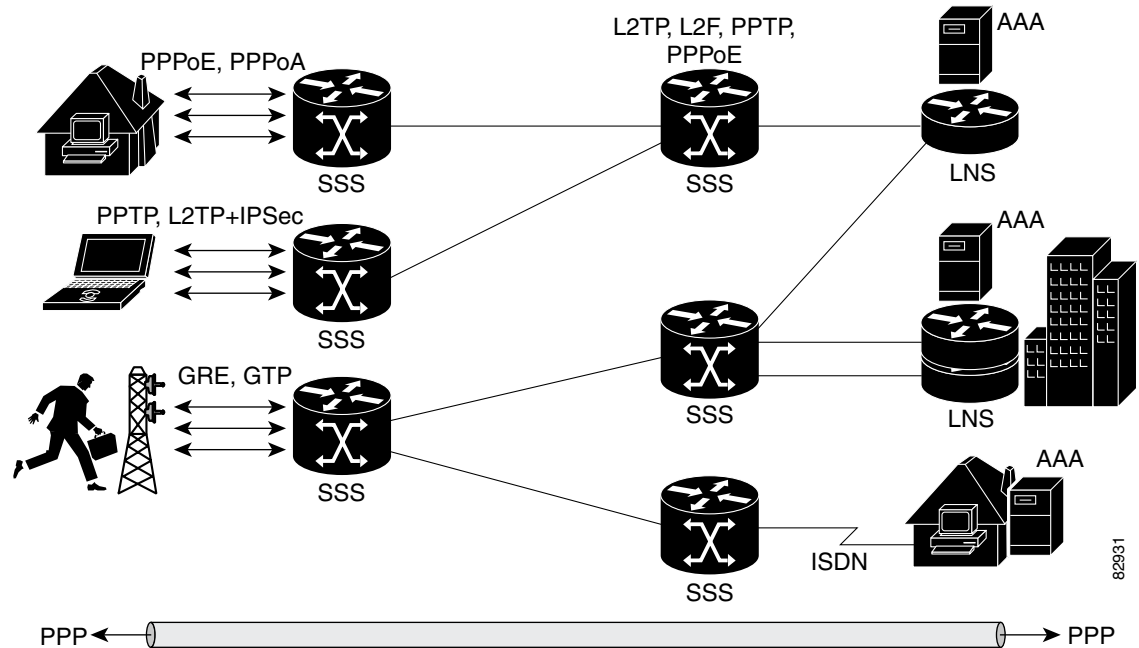
Benefits of Subscriber Service Switch

The Subscriber Service Switch was developed in response to a need by Internet service providers for increased scalability and extensibility for remote access service selection and Layer 2 subscriber policy management. This Layer 2 subscriber policy is needed to manage tunneling of PPP in a policy-based bridging fashion.

Subscriber Service Switch provides flexibility on where and how many subscribers are connected to available services and how those services are defined. In the past, remote access service selection was largely determined by the telephone number dialed or the PPP username and password entered during a PPP authentication cycle. However, emerging broadband, cable, Virtual Private Network (VPN), and wireless access methods have created an environment where PPP sessions may be tunneled over a variety of protocols and media. The multitude of protocols, management domains, network infrastructure, and variety of services has created a complex environment for directing a subscriber to a given service or application. The problem is further augmented by the much greater density of total PPP sessions that can be transported over shared media versus traditional point-to-point links. Subscriber Service Switch can provide a flexible and extensible decision point linking an incoming subscriber (typically a PPP session over some physical or virtual link) to another tunneled link or local termination for Layer 3 processing.

Subscriber Service Switch is also scalable in situations where a subscriber's Layer 2 service is switched across virtual links. Examples include switching between PPPoA, PPPoE, L2TP, Layer 2 Forwarding Protocol (L2F), Point-to-Point Tunneling Protocol (PPTP), generic routing encapsulation (GRE) and General Packet Radio Service (GPRS) Tunneling Protocol (GTP wireless data standard).

[Figure 1](#) shows how Subscriber Service Switch provides its own centralized switching path that bypasses the virtual access-based switching available in software prior to Cisco IOS Release 12.2(13)T. In the figure, Subscriber Service Switch is switching data traffic from personal computers in a home and corporate office, and from a wireless user.

Figure 1 BASIC Subscriber Service Switch Operation

Protocols that register with the Subscriber Service Switch application programming interface (API) can take advantage of this new switching path. Bypassing the virtual access interface in this manner helps the Cisco IOS software to scale to the increased number of sessions that the market demands today. Subscriber Service Switch also markedly improves network performance, too. For example, benchmark testing indicates that performance of L2TP multihop tasks occurs twice as fast in networks with Subscriber Service Switch versus networks without it.

Backward Compatibility

All of the current virtual private dialup network (VPDN), Multichassis Multilink PPP (MMLP), and local termination policies and configurations will be maintained in this implementation of Subscriber Service Switch; however, default policies may be overridden by the following configurations or events:

- Resource Manager (RM) VPDN authorization is attempted before VPDN authorization.
- VPDN authorization is attempted before Stack Group Forwarding (SGF) MMLP.
- VPDN service authorization is attempted only when the **vpdn enable** command is configured.
- RM VPDN service authorization is attempted only if RM is enabled.
- SGF authorization is attempted only when the **sgbp member** command is configured and one or both of the following service keys are available from the subscriber: unauthenticated PPP name and endpoint discriminator.
- The **dnis** and **domain** service keys, in that order, are used to authorize VPDN service, provided that VPDN service is enabled. The order may be changed with the **vpdn search-order** global command, which may include **multihop-hostname** as a service key.
- An unauthenticated PPP name is always reduced to a domain name by taking all characters from the right of the PPP name up to a configurable delimiter character (default is the @ character). Only the domain portion is used to locate a service.

- If the **vpdn authen-before-forward** command is configured as a global configuration command, the authenticated PPP name is used to authorize VPDN service.
- The configuration defined by the **vpdn-group** command can specify four things:
 1. Authorization for VPDN call termination (using the **accept-dialin** and **accept-dialout** keywords).
 2. Authorization for VPDN subscriber service (using the **request-dialin** and **request-dialout** keywords).
 3. A directive to collect further service keys and reauthorize (using the **authen-before-forward** keyword).
 4. A tunnel configuration.

Subscriber Service Switch adds a general configuration framework to replace the first three aspects of a VPDN group.

- If VPDN and SGF services either are not configured or cannot be authorized, local PPP termination service is selected. Further PPP authorization is still required to complete local termination.
- A two-phase authorization scheme is enabled by the **vpn domain authorization** command. An NAS-Port-ID (NAS port identifier) key is used to locate the first service record, which contains a restricted set of values for the domain substring of the unauthenticated PPP name. This filtered service key then locates the final service. Cisco refers to this scheme as *domain preauthorization*.
- Domain preauthorization will occur only when the NAS-Port-ID key is available.
- When domain preauthorization is enabled, both authenticated and unauthenticated domain names are checked for restrictions.
- It is possible to associate a fixed service with an ATM permanent virtual circuit (PVC), thus affecting any subscribers carried by the PVC. The **vpn service** command, in ATM VC or VC class configuration mode, and the associated key make up the generic service key.
- When the generic service key is available, it will be used for authorization instead of the unauthenticated domain name.
- If either the **vpdn authen-before-forward** or **per vpdn-group authen-before-forward** command is configured, the authenticated username is required and will be used to authorize VPDN service.
- To determine whether the **authen-before-forward** command is configured in a VPDN group (using the **vpdn-group** command), an unauthenticated username or the generic service key is required as the initial-want key set.
- When the global **vpdn authen-before-forward** command is not configured, the generic service key, if one is available, is used to determine whether the **authen-before-forward** function is configured in the VPDN group (using the **vpdn-group** command). If the generic service key is not available, the unauthenticated username will be used.
- If an accounting-enabled key is available, the unauthenticated username is required.
- VPDN multihop is allowed only when VPDN multihop is enabled.
- SGF on the L2TP network server (LNS) is allowed only when VPDN multihop is enabled on the LNS.
- Forwarding of SGF calls on the LAC is only allowed if VPDN multihop is enabled on the LAC.
- SGF-to-SGF multihop is not allowed.
- When PPP forwarding is configured, both MLP and non-MLP calls are forwarded to the winner of the Stack Group Bidding Protocol (SGBP) bid.
- Authentication is always required for forwarded Packet Data Serving Node (PDSN) calls.

- When the **directed-request** function is enabled and activated using the **ip host** command (legacy behavior), VPDN service authorization occurs only when the **vpdn authorize directed-request** function is enabled.
- Fixed legacy policy is still maintained for RM.

How to Use Subscriber Service Switch

The Subscriber Service Switch architecture is transparent, and existing PPP, VPDN, PPPoE, PPPoA, and authentication, authorization, and accounting (AAA) call configurations will continue to work in this new environment. You can, however, enable Subscriber Service Switch preauthorization and Subscriber Service Switch type authorization. You may also find it helpful to verify Subscriber Service Switch call operation.

This section contains the following optional procedures:

- [Enabling Domain Preauthorization on a LAC, page 5](#) (optional)
- [Enabling Subscriber Service Switch Preauthorization, page 7](#)(optional)
- [Verifying Subscriber Service Switch Call Operation, page 7](#) (optional)
- [Troubleshooting the Subscriber Service Switch, page 8](#) (optional)

Enabling Domain Preauthorization on a LAC

To enable the LAC to perform domain authorization before tunneling, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn authorize domain**
4. **exit**
5. **show running-config**
6. Create a RADIUS user profile for domain preauthorization

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	vpdn authorize domain Example: Router(config)# vpdn authorize domain	Enables domain preauthorization on a NAS.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.
Step 5	show running-config Example: Router# show running-config	Displays the configuration so you can check that you successfully enabled domain preauthorization.
Step 6	Create a RADIUS user profile for domain preauthorization.	—

What to Do Next

See the next section and the “Domain Preauthorization RADIUS User Profile Example” on page 11.

Creating a RADIUS User Profile for Domain Preauthorization

Table 1 lists the attributes to enable domain preauthorization in a RADIUS user profile. Refer to the [Cisco IOS Security Configuration Guide](#), Release 12.2, for information about creating a RADIUS user profile.

Table 1 Attributes for the RADIUS User Profile for Domain Preauthorization

RADIUS Entry	Purpose
nas-port: <i>ip-address:slot/subslot/port/vpi.vci</i>	Configures the NAS port username for domain preauthorization. <ul style="list-style-type: none"> <i>ip-address</i>—Management IP address of the node switch processor (NSP). <i>slot/subslot/port</i>—Specify ATM interface. <i>vpi.vci</i>—Virtual path identifier (VPI) and virtual channel identifier (VCI) values for the PVC.
Password = "cisco"	Sets the fixed password.
User-Service-Type = Outbound-User	Configures the service-type as outbound.
Cisco-AVpair = "vpdn:vpn-domain-list=domain1, domain2,..."	Specifies the domains accessible to the user. <ul style="list-style-type: none"> <i>domain</i>—Domain to configure as accessible to the user.


Enabling Subscriber Service Switch Preauthorization

When Subscriber Service Switch preauthorization is enabled on a LAC, local configurations for session limit per VC and per VLAN are overwritten by the per-NAS-port session limit downloaded from the server. To enable this preauthorization, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber access {pppoe | pppoa} pre-authorize nas-port-id [aaa-method-list]**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	subscriber access {pppoe pppoa} pre-authorize nas-port-id [aaa-method-list] Example: Router(config)# subscriber access pppoe pre-authorize nas-port-id mlist_llid	Enables Subscriber Service Switch preauthorization.  Note The LACs maintains a current session number per NAS port. As a new session request comes in, the LAC makes a preauthorization request to AAA to get the session limit, and compares it with the number of sessions currently on that NAS port. This command ensures that session limit querying is only enabled for PPPoE-type calls, not for any other call types.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.

Verifying Subscriber Service Switch Call Operation

To verify that the Subscriber Service Switch is working, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show sss session [all]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show sss session [all]	Displays Subscriber Service Switch session status.
	Example: Router# show sss session all	<ul style="list-style-type: none"> Use the optional all keyword to display an extensive report about the Subscriber Service Switch sessions.

What to Do Next

Information about troubleshooting a network running the Subscriber Service Switch can be found in the following “[Troubleshooting the Subscriber Service Switch](#), page 8 section.

Troubleshooting the Subscriber Service Switch

This section provides troubleshooting tips for the Subscriber Service Switch. Examples of normal and failure operations can be found in “[Troubleshoot Subscriber Service Switch Examples](#)” section on page 14. Reports from **debug** commands should be sent to technical personnel at Cisco Systems for evaluation.

Debug Commands Available for Subscriber Service Switch

The Subscriber Service Switch feature introduces five new EXEC mode **debug** commands to enable diagnostic output about Subscriber Service Switch call operation, as follows:

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

These commands were designed to be used with Cisco IOS **debug** commands that exist for troubleshooting PPP and other Layer 2 call operations. [Table 2](#) lists some of these **debug** commands.

Table 2 *Additional Debugging Commands for Troubleshooting Subscriber Service Switch*

Command	Purpose
debug pppoe events	Displays protocol event information.
debug pppoe errors	Displays PPPoE error messages.
debug ppp negotiation	Allows you to check that a client is passing PPP negotiation information.
debug vpdn l2x-events	Displays L2F and L2TP events that are part of tunnel establishment or shutdown.
debug vpdn l2x-errors	Displays L2F and L2TP protocol errors that prevent tunnel establishment or normal operation.
debug vpdn sss events	Displays diagnostic information about VPDN Subscriber Service Switch call setup events.
debug vpdn sss errors	Displays diagnostic information about errors that may occur during VPDN Subscriber Service Switch call setup.
debug vpdn call events	Enables VPDN call event debugging.
debug vpdn call fsm	Enables VPDN call setup state debugging.
debug vpdn events	Displays PPTP tunnel event change information.
debug vpdn errors	Displays PPTP protocol error messages.

**Note**

The commands are intended only for troubleshooting purposes, because the volume of output generated by the software can result in severe performance degradation on the router.


Troubleshoot the Subscriber Service Switch

To troubleshoot a network running the Subscriber Service Switch, perform the following steps:

SUMMARY STEPS

1. Attach a console directly to a router running the Cisco IOS Release 12.2(13)T or a later release.
2. **enable**
3. **configure terminal**
4. **no logging console**
5. Use Telnet to access a router port and repeat Steps 2 and 3.
6. **terminal monitor**
7. **exit**
8. **debug *command***
9. **configure {terminal | memory | network}**
10. **no terminal monitor**
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Attach a console directly to a router running the Cisco IOS Release 12.2(13)T or a later release.	—
Step 2	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	no logging console Example: Router(config)# no logging console	Disables all logging to the console terminal. To reenabling logging to the console, use the logging console command in global configuration mode.
Step 5	Use Telnet to access a router port and repeat Steps 2 and 3.	Enters global configuration mode in a recursive Telnet session, which allows the output to be redirected away from the console port.
Step 6	terminal monitor Example: Router(config)# terminal monitor	Enables logging output on the virtual terminal.
Step 7	exit Example: Router(config)# exit	Exits to privileged EXEC mode.
Step 8	debug command Example: Router# debug sss error Router# debug sss event Router# debug sss fsm	Enables the debug command. See “Debug Commands Available for Subscriber Service Switch” and Table 2 for commands that can be entered.
		 Note You can enter more than one debug command.
Step 9	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 10	no terminal monitor Example: Router(config)# no terminal monitor	Disables logging on the virtual terminal.
Step 11	exit Example: Router(config)# exit	Exits to privileged EXEC mode.

Configuration Examples for Subscriber Service Switch

This section provides the following configuration examples:

- [Enable LAC Domain Authorization Example, page 11](#)
- [Domain Preauthorization RADIUS User Profile Example, page 11](#)
- [Enable Subscriber Service Switch Preauthorization Example, page 12](#)
- [Verify Subscriber Service Switch Call Operation Example, page 12](#)
- [Troubleshoot Subscriber Service Switch Examples, page 14](#)

Enable LAC Domain Authorization Example

The following example shows the configuration necessary for the 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 typical 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
    }
  }
}
```

```

}
}
}

```

Enable Subscriber Service Switch Preauthorization Example

The following partial example signals Subscriber Service Switch to preauthorize the NAS-Port-ID string before authorizing the domain name. This policy applies only to all sessions with a PPPoE access type.

```

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
!

```

Verify Subscriber Service Switch Call Operation Example

The following example command output from the **show sss session all** command provides an extensive report of Subscriber Service Switch session activity. The text in bold shows the unique identifier for each session, which can be used to correlate that particular session with the session information retrieved from other **show** commands or **debug** command traces. See the following **show vpdn session** command output for an example of this unique ID correlation.

```
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@xyz.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@xyz.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@xyz.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@domain.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@xyz.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 useruser
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@<domain>.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

Correlating the Unique ID in show vpdn session all Command Output

The following partial sample output from the **show vpdn session all** command provides extensive reports on call activity for all L2TP, L2F, and PPPoE sessions, and identifies the unique ID for each session.

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 nobody3@xyz.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 nobody3@xyz.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

```

```

.
.
.

```

Troubleshoot Subscriber Service Switch Examples

This section provides the following debugging session examples for a network running the Subscriber Service Switch:

- [Troubleshoot the Subscriber Service Switch Operation Example, page 15](#)
- [Troubleshoot the Subscriber Service Switch on the LAC—Normal Operation Example, page 16](#)
- [Troubleshoot the Subscriber Service Switch on the LAC—Authorization Failure Example, page 18](#)
- [Troubleshoot the Subscriber Service Switch on the LAC—Authentication Failure Example, page 20](#)
- [Troubleshoot the Subscriber Service Switch at the LNS—Normal Operation Example, page 23](#)
- [Troubleshoot the Subscriber Service Switch at the LNS—Tunnel Failure Example, page 25](#)



Note

Reports from **debug** commands should be sent to technical personnel at Cisco Systems for evaluation.

Troubleshoot the Subscriber Service Switch Operation Example

The following example shows the **debug** commands used and sample output for debugging Subscriber Service Switch operation:

```
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
nobody@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

```

Troubleshoot the Subscriber Service Switch on the LAC—Normal Operation Example

The following example shows the **debug** commands used and sample output indicating normal operation of the Subscriber Service Switch on the LAC:

```

Router# debug sss event
Router# debug sss error
Router# debug sss aaa authorization event
Router# debug sss aaa authorization fsm
Router# debug pppoe events
Router# debug pppoe errors
Router# debug ppp negotiation
Router# debug vpdn l2x-events
Router# debug vpdn l2x-errors
Router# debug vpdn sss events
Router# debug vpdn sss errors
Router# debug vpdn call events
Router# debug vpdn call fsm
Router# debug vpdn events
Router# debug vpdn errors

```

SSS:

```

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

```

PPPoE:

```

  PPPoE protocol events debugging is on
  PPPoE protocol errors debugging is on

```

PPP:

```

  PPP protocol negotiation debugging is on

```

VPN:

```

  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN SSS events debugging is on
  VPDN SSS errors debugging is on
  VPDN call event debugging is on
  VPDN call FSM debugging is on
  VPDN events debugging is on
  VPDN errors debugging is on

```

```

*Nov 15 12:23:52.523: PPPoE 0: I PADI R:0000.0c14.71d0 L:ffff.ffff.ffff 1/32
ATM4/0.132
*Nov 15 12:23:52.523: PPPoE 0: O PADO R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:23:52.527: PPPoE 0: I PADR R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:23:52.527: PPPoE : encaps string prepared
*Nov 15 12:23:52.527: [13]PPPoE 10: Access IE handle allocated
*Nov 15 12:23:52.527: [13]PPPoE 10: pppoe SSS switch updated

```



```
*Nov 15 12:23:52.527: [13]PPPoE 10: Service request sent to SSS
*Nov 15 12:23:52.527: [13]PPPoE 10: Created R:00b0.c2e9.c870 L:0000.0c14.71d0 1/32
ATM4/0.132
*Nov 15 12:23:52.547: SSS INFO: Element type is Access-Type, long value is 3
*Nov 15 12:23:52.547: SSS INFO: Element type is Switch-Id, long value is 2130706444
*Nov 15 12:23:52.547: SSS INFO: Element type is Nasport, ptr value is 63C07288
*Nov 15 12:23:52.547: SSS INFO: Element type is AAA-Id, long value is 14
*Nov 15 12:23:52.547: SSS INFO: Element type is AccIe-Hdl, ptr value is B200000C
*Nov 15 12:23:52.547: SSS MGR [uid:13]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:23:52.547: SSS PM [uid:13]: RM/VPDN disabled: RM/VPDN author not needed
*Nov 15 12:23:52.547: SSS PM [uid:13]: Received Service Request
*Nov 15 12:23:52.547: SSS PM [uid:13]: Handling Authorization Check
*Nov 15 12:23:52.547: SSS PM [uid:13]: Policy requires 'Unauth-User' key
*Nov 15 12:23:52.547: SSS PM [uid:13]: Policy reply - Need more keys
*Nov 15 12:23:52.547: SSS MGR [uid:13]: Got reply Need-More-Keys from PM
*Nov 15 12:23:52.547: SSS MGR [uid:13]: Handling More-Keys event
*Nov 15 12:23:52.547: [13]PPPoE 10: State REQ_NASPORT      Event MORE_KEYS
*Nov 15 12:23:52.547: [13]PPPoE 10: O PADS R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:23:52.547: ppp13 PPP: Using default call direction
*Nov 15 12:23:52.547: ppp13 PPP: Treating connection as a dedicated line
*Nov 15 12:23:52.547: ppp13 PPP: Phase is ESTABLISHING, Active Open
*Nov 15 12:23:52.547: ppp13 LCP: O CONFREQ [Closed] id 1 len 19
*Nov 15 12:23:52.547: ppp13 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:23:52.547: ppp13 LCP:      AuthProto CHAP (0x0305C22305)
*Nov 15 12:23:52.547: ppp13 LCP:      MagicNumber 0xB0EC4557 (0x0506B0EC4557)
*Nov 15 12:23:52.547: [13]PPPoE 10: State START_PPP      Event DYN_BIND
*Nov 15 12:23:52.547: [13]PPPoE 10: data path set to PPP
*Nov 15 12:23:52.571: ppp13 LCP: I CONFREQ [REQsent] id 1 len 14
*Nov 15 12:23:52.571: ppp13 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:23:52.571: ppp13 LCP:      MagicNumber 0x0017455D (0x05060017455D)
*Nov 15 12:23:52.571: ppp13 LCP: O CONFACK [REQsent] id 1 len 14
*Nov 15 12:23:52.571: ppp13 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:23:52.571: ppp13 LCP:      MagicNumber 0x0017455D (0x05060017455D)
*Nov 15 12:23:54.543: ppp13 LCP: TIMEOUT: State ACKsent
*Nov 15 12:23:54.543: ppp13 LCP: O CONFREQ [ACKsent] id 2 len 19
*Nov 15 12:23:54.543: ppp13 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:23:54.543: ppp13 LCP:      AuthProto CHAP (0x0305C22305)
*Nov 15 12:23:54.543: ppp13 LCP:      MagicNumber 0xB0EC4557 (0x0506B0EC4557)
*Nov 15 12:23:54.543: ppp13 LCP: I CONFACK [ACKsent] id 2 len 19
*Nov 15 12:23:54.543: ppp13 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:23:54.543: ppp13 LCP:      AuthProto CHAP (0x0305C22305)
*Nov 15 12:23:54.543: ppp13 LCP:      MagicNumber 0xB0EC4557 (0x0506B0EC4557)
*Nov 15 12:23:54.543: ppp13 LCP: State is Open
*Nov 15 12:23:54.543: ppp13 PPP: Phase is AUTHENTICATING, by this end
*Nov 15 12:23:54.543: ppp13 CHAP: O CHALLENGE id 1 len 25 from "7200"
*Nov 15 12:23:54.547: ppp13 CHAP: I RESPONSE id 1 len 38 from "nobody@xyz.com"
*Nov 15 12:23:54.547: ppp13 PPP: Phase is FORWARDING, Attempting Forward
*Nov 15 12:23:54.547: SSS INFO: Element type is Unauth-User, string value is
nobody@xyz.com
*Nov 15 12:23:54.547: SSS INFO: Element type is AccIe-Hdl, ptr value is B200000C
*Nov 15 12:23:54.547: SSS INFO: Element type is AAA-Id, long value is 14
*Nov 15 12:23:54.547: SSS INFO: Element type is Access-Type, long value is 0
*Nov 15 12:23:54.547: SSS MGR [uid:13]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:23:54.547: SSS PM [uid:13]: Received More Keys
*Nov 15 12:23:54.547: SSS PM [uid:13]: Handling Authorization Check
*Nov 15 12:23:54.547: SSS PM [uid:13]: Handling AAA service Authorization
*Nov 15 12:23:54.547: SSS PM [uid:13]: Sending authorization request for 'xyz.com'

*Nov 15 12:23:54.547: SSS AAA AUTHOR [uid:13]:Event <make request>, state changed
from idle to authorizing
*Nov 15 12:23:54.547: SSS AAA AUTHOR [uid:13]:Authorizing key xyz.com
```

```

*Nov 15 12:23:54.547: SSS AAA AUTHOR [uid:13]:AAA request sent for key xyz.com
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Received an AAA pass
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Event <found service>, state changed
from authorizing to complete
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Found service info for key xyz.com
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Event <free request>, state changed
from complete to terminal
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Free request
*Nov 15 12:23:54.551: SSS PM [uid:13]: Handling Service Direction
*Nov 15 12:23:54.551: SSS PM [uid:13]: Policy reply - Forwarding
*Nov 15 12:23:54.551: SSS MGR [uid:13]: Got reply Forwarding from PM
*Nov 15 12:23:54.551: SSS MGR [uid:13]: Handling Connect-Service event
*Nov 15 12:23:54.551: VPDN CALL [uid:13]: Event connect req, state changed from idle
to connecting
*Nov 15 12:23:54.551: VPDN CALL [uid:13]: Requesting connection
*Nov 15 12:23:54.551: VPDN CALL [uid:13]: Call request sent
*Nov 15 12:23:54.551: VPDN MGR [uid:13]: Event client connect, state changed from
idle to connecting
*Nov 15 12:23:54.551: VPDN MGR [uid:13]: Initiating compulsory connection to
199.11.8.2
*Nov 15 12:23:54.551: Tnl/Sn61510/7 L2TP: Session FS enabled
*Nov 15 12:23:54.551: Tnl/Sn61510/7 L2TP: Session state change from idle to
wait-for-tunnel
*Nov 15 12:23:54.551: uid:13 Tnl/Sn61510/7 L2TP: Create session
*Nov 15 12:23:54.551: uid:13 Tnl/Sn61510/7 L2TP: O ICRQ to rp1 9264/0
*Nov 15 12:23:54.551: [13]PPPoE 10: Access IE nas port called
*Nov 15 12:23:54.555: Tnl61510 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:23:54.555: uid:13 Tnl/Sn61510/7 L2TP: Session state change from
wait-for-tunnel to wait-reply
*Nov 15 12:23:54.555: [13]PPPoE 10: State LCP_NEGO Event PPP_FWDING
*Nov 15 12:23:54.559: uid:13 Tnl/Sn61510/7 L2TP: O ICCN to rp1 9264/13586
*Nov 15 12:23:54.559: Tnl61510 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:23:54.559: uid:13 Tnl/Sn61510/7 L2TP: Session state change from
wait-reply to established
*Nov 15 12:23:54.559: uid:13 Tnl/Sn61510/7 L2TP: VPDN session up
*Nov 15 12:23:54.559: VPDN MGR [uid:13]: Event peer connected, state changed from
connecting to connected
*Nov 15 12:23:54.559: VPDN MGR [uid:13]: Succeed to forward nobody@xyz.com
*Nov 15 12:23:54.559: VPDN MGR [uid:13]: accounting start sent
*Nov 15 12:23:54.559: VPDN CALL [uid:13]: Event connect ok, state changed from
connecting to connected
*Nov 15 12:23:54.559: VPDN CALL [uid:13]: Connection succeeded
*Nov 15 12:23:54.559: SSS MGR [uid:13]: Handling Service-Connected event
*Nov 15 12:23:54.559: ppp13 PPP: Phase is FORWARDED, Session Forwarded
*Nov 15 12:23:54.559: [13]PPPoE 10: State LCP_NEGO Event PPP_FWDED
*Nov 15 12:23:54.563: [13]PPPoE 10: data path set to SSS Switch
*Nov 15 12:23:54.563: [13]PPPoE 10: Connected Forwarded

```

Troubleshoot the Subscriber Service Switch on the LAC—Authorization Failure Example

The following is sample output indicating call failure due to authorization failure:

```

*Nov 15 12:37:24.535: PPPoE 0: I PADI R:0000.0c14.71d0 L:ffff.ffff.ffff 1/32
ATM4/0.132
*Nov 15 12:37:24.535: PPPoE 0: O PADO R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:24.539: PPPoE 0: I PADR R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:24.539: PPPoE : encaps string prepared
*Nov 15 12:37:24.539: [18]PPPoE 15: Access IE handle allocated
*Nov 15 12:37:24.539: [18]PPPoE 15: pppoe SSS switch updated

```

```
*Nov 15 12:37:24.539: PPPoE 15: AAA pppoe_aaa_acct_get_retrieved_attrs
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_nas_port_details
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA unique ID allocated
*Nov 15 12:37:24.539: [18]PPPoE 15: No AAA accounting method list
*Nov 15 12:37:24.539: [18]PPPoE 15: Service request sent to SSS
*Nov 15 12:37:24.539: [18]PPPoE 15: Created R:00b0.c2e9.c870 L:0000.0c14.71d0 1/32
ATM4/0.132
*Nov 15 12:37:24.559: SSS INFO: Element type is Access-Type, long value is 3
*Nov 15 12:37:24.559: SSS INFO: Element type is Switch-Id, long value is -738197487
*Nov 15 12:37:24.559: SSS INFO: Element type is Nasport, ptr value is 63C0E590
*Nov 15 12:37:24.559: SSS INFO: Element type is AAA-Id, long value is 19
*Nov 15 12:37:24.559: SSS INFO: Element type is AccIe-Hdl, ptr value is 5B000011
*Nov 15 12:37:24.559: SSS MGR [uid:18]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:37:24.559: SSS PM [uid:18]: RM/VPDN disabled: RM/VPDN author not needed
*Nov 15 12:37:24.559: SSS PM [uid:18]: Received Service Request
*Nov 15 12:37:24.559: SSS PM [uid:18]: Handling Authorization Check
*Nov 15 12:37:24.559: SSS PM [uid:18]: Policy requires 'Unauth-User' key
*Nov 15 12:37:24.559: SSS PM [uid:18]: Policy reply - Need more keys
*Nov 15 12:37:24.559: SSS MGR [uid:18]: Got reply Need-More-Keys from PM
*Nov 15 12:37:24.559: SSS MGR [uid:18]: Handling More-Keys event
*Nov 15 12:37:24.559: [18]PPPoE 15: State REQ_NASPORT Event MORE_KEYS
*Nov 15 12:37:24.559: [18]PPPoE 15: O PADS R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:24.559: ppp18 PPP: Using default call direction
*Nov 15 12:37:24.559: ppp18 PPP: Treating connection as a dedicated line
*Nov 15 12:37:24.559: ppp18 PPP: Phase is ESTABLISHING, Active Open
*Nov 15 12:37:24.559: ppp18 LCP: O CONFREQ [Closed] id 1 len 19
*Nov 15 12:37:24.559: ppp18 LCP: MRU 1492 (0x010405D4)
*Nov 15 12:37:24.559: ppp18 LCP: AuthProto CHAP (0x0305C22305)
*Nov 15 12:37:24.559: ppp18 LCP: MagicNumber 0xB0F8A971 (0x0506B0F8A971)
*Nov 15 12:37:24.559: [18]PPPoE 15: State START_PPP Event DYN_BIND
*Nov 15 12:37:24.559: [18]PPPoE 15: data path set to PPP
*Nov 15 12:37:24.563: ppp18 LCP: I CONFREQ [REQsent] id 1 len 14
*Nov 15 12:37:24.563: ppp18 LCP: MRU 1492 (0x010405D4)
*Nov 15 12:37:24.563: ppp18 LCP: MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:24.563: ppp18 LCP: O CONFACK [REQsent] id 1 len 14
*Nov 15 12:37:24.563: ppp18 LCP: MRU 1492 (0x010405D4)
*Nov 15 12:37:24.563: ppp18 LCP: MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:26.523: ppp18 LCP: I CONFREQ [ACKsent] id 2 len 14
*Nov 15 12:37:26.523: ppp18 LCP: MRU 1492 (0x010405D4)
*Nov 15 12:37:26.523: ppp18 LCP: MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:26.523: ppp18 LCP: O CONFACK [ACKsent] id 2 len 14
*Nov 15 12:37:26.527: ppp18 LCP: MRU 1492 (0x010405D4)
*Nov 15 12:37:26.527: ppp18 LCP: MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:26.575: ppp18 LCP: TIMEOUT: State ACKsent
*Nov 15 12:37:26.575: ppp18 LCP: O CONFREQ [ACKsent] id 2 len 19
*Nov 15 12:37:26.575: ppp18 LCP: MRU 1492 (0x010405D4)
*Nov 15 12:37:26.575: ppp18 LCP: AuthProto CHAP (0x0305C22305)
*Nov 15 12:37:26.575: ppp18 LCP: MagicNumber 0xB0F8A971 (0x0506B0F8A971)
*Nov 15 12:37:26.575: ppp18 LCP: I CONFACK [ACKsent] id 2 len 19
*Nov 15 12:37:26.575: ppp18 LCP: MRU 1492 (0x010405D4)
*Nov 15 12:37:26.575: ppp18 LCP: AuthProto CHAP (0x0305C22305)
*Nov 15 12:37:26.575: ppp18 LCP: MagicNumber 0xB0F8A971 (0x0506B0F8A971)
*Nov 15 12:37:26.575: ppp18 LCP: State is Open
*Nov 15 12:37:26.575: ppp18 PPP: Phase is AUTHENTICATING, by this end
*Nov 15 12:37:26.575: ppp18 CHAP: O CHALLENGE id 1 len 25 from "7200"
*Nov 15 12:37:26.579: ppp18 CHAP: I RESPONSE id 1 len 38 from "nobody@xyz.com"
*Nov 15 12:37:26.579: ppp18 PPP: Phase is FORWARDING, Attempting Forward
*Nov 15 12:37:26.579: SSS INFO: Element type is Unauth-User, string value is
nobody@xyz.com
*Nov 15 12:37:26.579: SSS INFO: Element type is AccIe-Hdl, ptr value is 5B000011
```

```

*Nov 15 12:37:26.579: SSS INFO: Element type is AAA-Id, long value is 19
*Nov 15 12:37:26.579: SSS INFO: Element type is Access-Type, long value is 0
*Nov 15 12:37:26.579: SSS MGR [uid:18]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:37:26.579: SSS PM [uid:18]: Received More Keys
*Nov 15 12:37:26.579: SSS PM [uid:18]: Handling Authorization Check
*Nov 15 12:37:26.579: SSS PM [uid:18]: Handling AAA service Authorization
*Nov 15 12:37:26.579: SSS PM [uid:18]: Sending authorization request for 'xyz.com'

*Nov 15 12:37:26.579: SSS AAA AUTHOR [uid:18]:Event <make request>, state changed
from idle to authorizing
*Nov 15 12:37:26.579: SSS AAA AUTHOR [uid:18]:Authorizing key xyz.com
*Nov 15 12:37:26.579: SSS AAA AUTHOR [uid:18]:AAA request sent for key xyz.com
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Received an AAA failure
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Event <service not found>, state
changed from authorizing to complete
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:No service authorization info found
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Event <free request>, state changed
from complete to terminal
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Free request
*Nov 15 12:37:26.587: SSS PM [uid:18]: Handling Next Authorization Check
*Nov 15 12:37:26.587: SSS PM [uid:18]: Default policy: SGF author not needed
*Nov 15 12:37:26.587: SSS PM [uid:18]: Handling Default Service
*Nov 15 12:37:26.587: SSS PM [uid:18]: Policy reply - Local terminate
*Nov 15 12:37:26.591: SSS MGR [uid:18]: Got reply Local-Term from PM
*Nov 15 12:37:26.591: SSS MGR [uid:18]: Handling Send-Client-Local-Term event
*Nov 15 12:37:26.591: ppp18 PPP: Phase is AUTHENTICATING, Unauthenticated User
*Nov 15 12:37:26.595: ppp18 CHAP: O FAILURE id 1 len 25 msg is "Authentication
failed"
*Nov 15 12:37:26.599: ppp18 PPP: Sending Acct Event[Down] id[13]
*Nov 15 12:37:26.599: ppp18 PPP: Phase is TERMINATING
*Nov 15 12:37:26.599: ppp18 LCP: O TERMREQ [Open] id 3 len 4
*Nov 15 12:37:26.599: ppp18 LCP: State is Closed
*Nov 15 12:37:26.599: ppp18 PPP: Phase is DOWN
*Nov 15 12:37:26.599: ppp18 PPP: Phase is TERMINATING
*Nov 15 12:37:26.599: [18]PPPoE 15: State LCP_NEGO      Event PPP_DISCNET
*Nov 15 12:37:26.599: [18]PPPoE 15: O PADT R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:26.599: [18]PPPoE 15: Destroying R:0000.0c14.71d0 L:00b0.c2e9.c870
1/32 ATM4/0.132
*Nov 15 12:37:26.599: [18]PPPoE 15: AAA account stopped
*Nov 15 12:37:26.599: SSS MGR [uid:18]: Processing a client disconnect
*Nov 15 12:37:26.599: SSS MGR [uid:18]: Handling Send-Service-Disconnect event

```

Troubleshoot the Subscriber Service Switch on the LAC—Authentication Failure Example

The following is sample output indicating call failure due to authentication failure at the LNS:

```

*Nov 15 12:45:02.067: PPPoE 0: I PADI R:0000.0c14.71d0 L:ffff.ffff.ffff 1/32
ATM4/0.132
*Nov 15 12:45:02.071: PPPoE 0: O PADO R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:02.071: PPPoE 0: I PADR R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:02.071: PPPoE : encaps string prepared
*Nov 15 12:45:02.071: [21]PPPoE 18: Access IE handle allocated
*Nov 15 12:45:02.071: [21]PPPoE 18: pppoe SSS switch updated
*Nov 15 12:45:02.071: PPPoE 18: AAA pppoe_aaa_acct_get_retrieved_attrs
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA pppoe_aaa_acct_get_nas_port_details
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA unique ID allocated
*Nov 15 12:45:02.071: [21]PPPoE 18: No AAA accounting method list

```

```
*Nov 15 12:45:02.071: [21]PPPoE 18: Service request sent to SSS
*Nov 15 12:45:02.071: [21]PPPoE 18: Created R:00b0.c2e9.c870 L:0000.0c14.71d0 1/32
ATM4/0.132
*Nov 15 12:45:02.091: SSS INFO: Element type is Access-Type, long value is 3
*Nov 15 12:45:02.091: SSS INFO: Element type is Switch-Id, long value is 1946157076
*Nov 15 12:45:02.091: SSS INFO: Element type is Nasport, ptr value is 63B34170
*Nov 15 12:45:02.091: SSS INFO: Element type is AAA-Id, long value is 22
*Nov 15 12:45:02.091: SSS INFO: Element type is AccIe-Hdl, ptr value is 71000014
*Nov 15 12:45:02.091: SSS MGR [uid:21]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:45:02.091: SSS PM [uid:21]: RM/VPDN disabled: RM/VPDN author not needed
*Nov 15 12:45:02.091: SSS PM [uid:21]: Received Service Request
*Nov 15 12:45:02.091: SSS PM [uid:21]: Handling Authorization Check
*Nov 15 12:45:02.091: SSS PM [uid:21]: Policy requires 'Unauth-User' key
*Nov 15 12:45:02.091: SSS PM [uid:21]: Policy reply - Need more keys
*Nov 15 12:45:02.091: SSS MGR [uid:21]: Got reply Need-More-Keys from PM
*Nov 15 12:45:02.091: SSS MGR [uid:21]: Handling More-Keys event
*Nov 15 12:45:02.091: [21]PPPoE 18: State REQ_NASPORT      Event MORE_KEYS
*Nov 15 12:45:02.091: [21]PPPoE 18: O PADS R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:02.091: ppp21 PPP: Using default call direction
*Nov 15 12:45:02.091: ppp21 PPP: Treating connection as a dedicated line
*Nov 15 12:45:02.091: ppp21 PPP: Phase is ESTABLISHING, Active Open
*Nov 15 12:45:02.091: ppp21 LCP: O CONFREQ [Closed] id 1 len 19
*Nov 15 12:45:02.091: ppp21 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:45:02.091: ppp21 LCP:      AuthProto CHAP (0x0305C22305)
*Nov 15 12:45:02.091: ppp21 LCP:      MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
*Nov 15 12:45:02.091: [21]PPPoE 18: State START_PPP      Event DYN_BIND
*Nov 15 12:45:02.091: [21]PPPoE 18: data path set to PPP
*Nov 15 12:45:02.095: ppp21 LCP: I CONFREQ [REQsent] id 1 len 14
*Nov 15 12:45:02.095: ppp21 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:45:02.095: ppp21 LCP:      MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:02.095: ppp21 LCP: O CONFACK [REQsent] id 1 len 14
*Nov 15 12:45:02.095: ppp21 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:45:02.095: ppp21 LCP:      MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:02.315:  Tnl41436 L2TP: I StopCCN from rpl tnl 31166
*Nov 15 12:45:02.315:  Tnl41436 L2TP: Shutdown tunnel
*Nov 15 12:45:02.315:  Tnl41436 L2TP: Tunnel state change from no-sessions-left to
idle
*Nov 15 12:45:04.055: ppp21 LCP: I CONFREQ [ACKsent] id 2 len 14
*Nov 15 12:45:04.055: ppp21 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:45:04.059: ppp21 LCP:      MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:04.059: ppp21 LCP: O CONFACK [ACKsent] id 2 len 14
*Nov 15 12:45:04.059: ppp21 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:45:04.059: ppp21 LCP:      MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:04.079: ppp21 LCP: TIMEOUT: State ACKsent
*Nov 15 12:45:04.079: ppp21 LCP: O CONFREQ [ACKsent] id 2 len 19
*Nov 15 12:45:04.079: ppp21 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:45:04.079: ppp21 LCP:      AuthProto CHAP (0x0305C22305)
*Nov 15 12:45:04.079: ppp21 LCP:      MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
*Nov 15 12:45:04.079: ppp21 LCP: I CONFACK [ACKsent] id 2 len 19
*Nov 15 12:45:04.079: ppp21 LCP:      MRU 1492 (0x010405D4)
*Nov 15 12:45:04.079: ppp21 LCP:      AuthProto CHAP (0x0305C22305)
*Nov 15 12:45:04.079: ppp21 LCP:      MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
*Nov 15 12:45:04.079: ppp21 LCP: State is Open
*Nov 15 12:45:04.079: ppp21 PPP: Phase is AUTHENTICATING, by this end
*Nov 15 12:45:04.079: ppp21 CHAP: O CHALLENGE id 1 len 25 from "7200"
*Nov 15 12:45:04.083: ppp21 CHAP: I RESPONSE id 1 len 38 from "nobody@xyz.com"
*Nov 15 12:45:04.083: ppp21 PPP: Phase is FORWARDING, Attempting Forward
*Nov 15 12:45:04.083: SSS INFO: Element type is Unauth-User, string value is
nobody@xyz.com
*Nov 15 12:45:04.083: SSS INFO: Element type is AccIe-Hdl, ptr value is 71000014
*Nov 15 12:45:04.083: SSS INFO: Element type is AAA-Id, long value is 22
*Nov 15 12:45:04.083: SSS INFO: Element type is Access-Type, long value is 0
```

```

*Nov 15 12:45:04.083: SSS MGR [uid:21]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:45:04.083: SSS PM [uid:21]: Received More Keys
*Nov 15 12:45:04.083: SSS PM [uid:21]: Handling Authorization Check
*Nov 15 12:45:04.083: SSS PM [uid:21]: Handling AAA service Authorization
*Nov 15 12:45:04.083: SSS PM [uid:21]: Sending authorization request for 'xyz.com'

*Nov 15 12:45:04.083: SSS AAA AUTHOR [uid:21]:Event <make request>, state changed
from idle to authorizing
*Nov 15 12:45:04.083: SSS AAA AUTHOR [uid:21]:Authorizing key xyz.com
*Nov 15 12:45:04.083: SSS AAA AUTHOR [uid:21]:AAA request sent for key xyz.com
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Received an AAA pass
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Event <found service>, state changed
from authorizing to complete
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Found service info for key xyz.com
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Event <free request>, state changed
from complete to terminal
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Free request
*Nov 15 12:45:04.095: SSS PM [uid:21]: Handling Service Direction
*Nov 15 12:45:04.095: SSS PM [uid:21]: Policy reply - Forwarding
*Nov 15 12:45:04.095: SSS MGR [uid:21]: Got reply Forwarding from PM
*Nov 15 12:45:04.099: SSS MGR [uid:21]: Handling Connect-Service event
*Nov 15 12:45:04.099: VPDN CALL [uid:21]: Event connect req, state changed from idle
to connecting
*Nov 15 12:45:04.099: VPDN CALL [uid:21]: Requesting connection
*Nov 15 12:45:04.099: VPDN CALL [uid:21]: Call request sent
*Nov 15 12:45:04.099: VPDN MGR [uid:21]: Event client connect, state changed from
idle to connecting
*Nov 15 12:45:04.099: VPDN MGR [uid:21]: Initiating compulsory connection to
199.11.8.2
*Nov 15 12:45:04.099: Tnl/Sn31399/10 L2TP: Session FS enabled
*Nov 15 12:45:04.099: Tnl/Sn31399/10 L2TP: Session state change from idle to
wait-for-tunnel
*Nov 15 12:45:04.099: uid:21 Tnl/Sn31399/10 L2TP: Create session
*Nov 15 12:45:04.099: Tnl31399 L2TP: SM State idle
*Nov 15 12:45:04.099: Tnl31399 L2TP: O SCCRQ
*Nov 15 12:45:04.099: Tnl31399 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:45:04.099: Tnl31399 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Nov 15 12:45:04.099: Tnl31399 L2TP: SM State wait-ctl-reply
*Nov 15 12:45:04.099: [21]PPPoE 18: State LCP_NEGO Event PPP_FWDING
*Nov 15 12:45:04.107: Tnl31399 L2TP: I SCCRP from rp1
*Nov 15 12:45:04.107: Tnl31399 L2TP: Got a challenge from remote peer, rp1
*Nov 15 12:45:04.107: Tnl31399 L2TP: Got a response from remote peer, rp1
*Nov 15 12:45:04.107: Tnl31399 L2TP: Tunnel Authentication success
*Nov 15 12:45:04.107: Tnl31399 L2TP: Tunnel state change from wait-ctl-reply to
established
*Nov 15 12:45:04.107: Tnl31399 L2TP: O SCCCN to rp1 tn1id 9349
*Nov 15 12:45:04.107: Tnl31399 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:45:04.107: Tnl31399 L2TP: SM State established
*Nov 15 12:45:04.107: uid:21 Tnl/Sn31399/10 L2TP: O ICRQ to rp1 9349/0
*Nov 15 12:45:04.107: [21]PPPoE 18: Access IE nas port called
*Nov 15 12:45:04.107: uid:21 Tnl/Sn31399/10 L2TP: Session state change from
wait-for-tunnel to wait-reply
*Nov 15 12:45:04.115: uid:21 Tnl/Sn31399/10 L2TP: O ICCN to rp1 9349/13589
*Nov 15 12:45:04.115: Tnl31399 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:45:04.115: uid:21 Tnl/Sn31399/10 L2TP: Session state change from
wait-reply to established
*Nov 15 12:45:04.115: uid:21 Tnl/Sn31399/10 L2TP: VPDN session up
*Nov 15 12:45:04.115: VPDN MGR [uid:21]: Event peer connected, state changed from
connecting to connected

```

```

*Nov 15 12:45:04.115: VPDN MGR [uid:21]: Succeed to forward nobody@xyz.com
*Nov 15 12:45:04.115: VPDN MGR [uid:21]: accounting start sent
*Nov 15 12:45:04.115: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.115: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.115: VPDN CALL [uid:21]: Event connect ok, state changed from
connecting to connected
*Nov 15 12:45:04.115: VPDN CALL [uid:21]: Connection succeeded
*Nov 15 12:45:04.115: SSS MGR [uid:21]: Handling Service-Connected event
*Nov 15 12:45:04.115: ppp21 PPP: Phase is FORWARDED, Session Forwarded
*Nov 15 12:45:04.115: [21]PPPoE 18: State LCP_NEGO      Event PPP_FWDED
*Nov 15 12:45:04.115: [21]PPPoE 18: data path set to SSS Switch
*Nov 15 12:45:04.119: [21]PPPoE 18: Connected Forwarded
*Nov 15 12:45:04.119: ppp21 PPP: Process pending packets
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: Result code(2): 2: Call
disconnected, refer to error msg
*Nov 15 12:45:04.139:      Error code(6): Vendor specific
*Nov 15 12:45:04.139:      Optional msg: Locally generated disconnect
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: I CDN from rp1 tnl 9349, c1
13589
01:06:21: %VPDN-6-CLOSED: L2TP LNS 199.11.8.2 closed  user nobody@xyz.com; Result
2, Error 6, Locally generated disconnect
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: disconnect (L2X) IETF:
18/host-request Ascend: 66/VPDN Local PPP Disconnect
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: Destroying session
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: Session state change from
established to idle
*Nov 15 12:45:04.139: VPDN MGR [uid:21]: Event peer disconnect, state changed from
connected to disconnected
*Nov 15 12:45:04.139: VPDN MGR [uid:21]: Remote disconnected nobody@xyz.com
*Nov 15 12:45:04.139: VPDN MGR [uid:21]: accounting stop sent
*Nov 15 12:45:04.139:  Tnl31399 L2TP: Tunnel state change from established to
no-sessions-left
*Nov 15 12:45:04.143:  Tnl31399 L2TP: No more sessions in tunnel, shutdown (likely)
in 15 seconds
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Event server disc, state changed from
connected to disconnected
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Server disconnected call
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Event free req, state changed from
disconnected to terminal
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Free request
*Nov 15 12:45:04.143: SSS MGR [uid:21]: Handling Send Client Disconnect
*Nov 15 12:45:04.143: [21]PPPoE 18: State CNCT_FWDED      Event SSS_DISCNCT
*Nov 15 12:45:04.143: ppp21 PPP: Sending Acct Event[Down] id[16]
*Nov 15 12:45:04.143: ppp21 PPP: Phase is TERMINATING
*Nov 15 12:45:04.143: ppp21 LCP: State is Closed
*Nov 15 12:45:04.143: ppp21 PPP: Phase is DOWN
*Nov 15 12:45:04.143: [21]PPPoE 18: O PADT R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:04.143: [21]PPPoE 18: Destroying R:0000.0c14.71d0 L:00b0.c2e9.c870
1/32 ATM4/0.132
*Nov 15 12:45:04.143: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.143: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.143: [21]PPPoE 18: AAA account stopped
*Nov 15 12:45:14.139:  Tnl31399 L2TP: I StopCCN from rp1 tnl 9349
*Nov 15 12:45:14.139:  Tnl31399 L2TP: Shutdown tunnel
*Nov 15 12:45:14.139:  Tnl31399 L2TP: Tunnel state change from no-sessions-left

```

Troubleshoot the Subscriber Service Switch at the LNS—Normal Operation Example

The following example shows the **debug** commands used and sample output indicating normal operation of the Subscriber Service Switch on the LNS:

```

Router# debug sss event
Router# debug sss error
Router# debug sss fsm
Router# debug ppp negotiation
Router# debug vpdn l2x-events
Router# debug vpdn l2x-errors
Router# debug vpdn sss events
Router# debug vpdn sss errors
Router# debug vpdn sss fsm

SSS:
  SSS events debugging is on
  SSS error debugging is on
  SSS fsm debugging is on
PPP:
  PPP protocol negotiation debugging is on

VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN SSS events debugging is on
  VPDN SSS errors debugging is on
  VPDN SSS FSM debugging is on

3d17h: Tnl9264 L2TP: I ICRQ from server1 tnl 61510
3d17h: Tnl/Sn9264/13586 L2TP: Session FS enabled
3d17h: Tnl/Sn9264/13586 L2TP: Session state change from idle to wait-connect
3d17h: Tnl/Sn9264/13586 L2TP: New session created
3d17h: Tnl/Sn9264/13586 L2TP: O ICRP to server1 61510/7
3d17h: Tnl9264 L2TP: Control channel retransmit delay set to 1 seconds
3d17h: Tnl/Sn9264/13586 L2TP: I ICCN from server1 tnl 61510, cl 7
3d17h: nobody@xyz.com Tnl/Sn9264/13586 L2TP: Session state change from
wait-connect to wait-for-service-selection
3d17h: VPDN SSS []: Event start sss, state changed from IDLE to SSS
3d17h: VPDN SSS [uid:707]: Service request sent to SSS
3d17h: SSS INFO: Element type is Access-Type, long value is 4
3d17h: SSS INFO: Element type is Switch-Id, long value is 1493172561
3d17h: SSS INFO: Element type is Tunnel-Name, string value is server1
3d17h: SSS INFO: Element type is Can-SIP-Redirect, long value is 1
3d17h: SSS INFO: Element type is AAA-Id, long value is 16726
3d17h: SSS INFO: Element type is AccIe-Hdl, ptr value is D1000167
3d17h: SSS MGR [uid:707]: Event service-request, state changed from wait-for-req to
wait-for-auth
3d17h: SSS MGR [uid:707]: Handling Policy Authorize (1 pending sessions)
3d17h: SSS PM [uid:707]: RM/VPDN disabled: RM/VPDN author not needed
3d17h: SSS PM [uid:707]: Multihop disabled: AAA author not needed
3d17h: SSS PM [uid:707]: Multihop disabled: SGF author not needed
3d17h: SSS PM [uid:707]: No more authorization methods left to try, providing
default service
3d17h: SSS PM [uid:707]: Received Service Request
3d17h: SSS PM [uid:707]: Event <found>, State: initial-req to end
3d17h: SSS PM [uid:707]: Handling Service Direction
3d17h: SSS PM [uid:707]: Policy reply - Local terminate
3d17h: SSS MGR [uid:707]: Got reply Local-Term from PM
3d17h: SSS MGR [uid:707]: Event policy-connect local, state changed from
wait-for-auth to connected
3d17h: SSS MGR [uid:707]: Handling Send-Client-Local-Term event
3d17h: VPDN SSS [uid:707]: Event connect local, state changed from SSS to PPP
3d17h: ppp707 PPP: Phase is ESTABLISHING
3d17h: ppp707 LCP: I FORCED rcvd CONFACK len 15
3d17h: ppp707 LCP: MRU 1492 (0x010405D4)
3d17h: ppp707 LCP: AuthProto CHAP (0x0305C22305)
3d17h: ppp707 LCP: MagicNumber 0xB0EC4557 (0x0506B0EC4557)
3d17h: ppp707 LCP: I FORCED sent CONFACK len 10

```



```

3d17h: ppp707 LCP:      MRU 1492 (0x010405D4)
3d17h: ppp707 LCP:      MagicNumber 0x0017455D (0x05060017455D)
3d17h: ppp707 PPP: Phase is FORWARDING, Attempting Forward
3d17h: VPDN SSS [uid:707]: Event dyn bind resp, state changed from PPP to PPP
3d17h: ppp707 PPP: Phase is AUTHENTICATING, Unauthenticated User
3d17h: ppp707 PPP: Phase is FORWARDING, Attempting Forward
3d17h: VPDN SSS [uid:707]: Event connect local, state changed from PPP to PPP
3d17h: VPDN SSS [Vi4.2]: Event vaccess resp, state changed from PPP to PPP
3d17h: VPDN SSS [Vi4.2]: Event stat bind resp, state changed from PPP to CNCT
3d17h: Vi4.2  Tnl/Sn9264/13586 L2TP: Session state change from
wait-for-service-selection to established
3d17h: Vi4.2 PPP: Phase is AUTHENTICATING, Authenticated User
3d17h: Vi4.2 CHAP: O SUCCESS id 1 len 4
3d17h: Vi4.2 PPP: Phase is UP
3d17h: Vi4.2 IPCP: O CONFREQ [Closed] id 1 len 10
3d17h: Vi4.2 IPCP:      Address 172.18.0.0 (0x030681010000)
3d17h: Vi4.2 PPP: Process pending packets
3d17h: Vi4.2 IPCP: I CONFREQ [REQsent] id 1 len 10
3d17h: Vi4.2 IPCP:      Address 0.0.0.0 (0x030600000000)
3d17h: Vi4.2 AAA/AUTHOR/PCP: Start.  Her address 0.0.0.0, we want 0.0.0.0
3d17h: Vi4.2 AAA/AUTHOR/PCP: Done.  Her address 0.0.0.0, we want 0.0.0.0
3d17h: Vi4.2 IPCP: Pool returned 10.1.1.3
3d17h: Vi4.2 IPCP: O CONFNAK [REQsent] id 1 len 10
3d17h: Vi4.2 IPCP:      Address 10.1.1.3 (0x03065B010103)
3d17h: Vi4.2 IPCP: I CONFACK [REQsent] id 1 len 10
3d17h: Vi4.2 IPCP:      Address 172.18.0.0 (0x030681010000)
3d17h: Vi4.2 IPCP: I CONFREQ [ACKrcvd] id 2 len 10
3d17h: Vi4.2 IPCP:      Address 10.1.1.3 (0x03065B010103)
3d17h: Vi4.2 IPCP: O CONFACK [ACKrcvd] id 2 len 10
3d17h: Vi4.2 IPCP:      Address 10.1.1.3 (0x03065B010103)
3d17h: Vi4.2 IPCP: State is Open
3d17h: Vi4.2 IPCP: Install route to 10.1.1.3

```

Troubleshoot the Subscriber Service Switch at the LNS—Tunnel Failure Example

The following is sample output indicating tunnel failure on the LNS:

```

3d17h: L2TP: I SCCRQ from server1 tnl 31399
3d17h:  Tnl9349 L2TP: Got a challenge in SCCRQ, server1
3d17h:  Tnl9349 L2TP: New tunnel created for remote server1, address 199.11.8.1
3d17h:  Tnl9349 L2TP: O SCCRP  to server1 tnlid 31399
3d17h:  Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h:  Tnl9349 L2TP: Tunnel state change from idle to wait-ctl-reply
3d17h:  Tnl9349 L2TP: I SCCCN from server1 tnl 31399
3d17h:  Tnl9349 L2TP: Got a Challenge Response in SCCCN from server1
3d17h:  Tnl9349 L2TP: Tunnel Authentication success
3d17h:  Tnl9349 L2TP: Tunnel state change from wait-ctl-reply to established
3d17h:  Tnl9349 L2TP: SM State established
3d17h:  Tnl9349 L2TP: I ICRQ from server1 tnl 31399
3d17h:  Tnl/Sn9349/13589 L2TP: Session FS enabled
3d17h:  Tnl/Sn9349/13589 L2TP: Session state change from idle to wait-connect
3d17h:  Tnl/Sn9349/13589 L2TP: New session created
3d17h:  Tnl/Sn9349/13589 L2TP: O ICRP to server1 31399/10
3d17h:  Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h:  Tnl/Sn9349/13589 L2TP: I ICCN from server1 tnl 31399, cl 10
3d17h: nobody@xyz.com  Tnl/Sn9349/13589 L2TP: Session state change from
wait-connect to wait-for-service-selection
3d17h: VPDN SSS []: Event start sss, state changed from IDLE to SSS
3d17h: VPDN SSS [uid:709]: Service request sent to SSS
3d17h: SSS INFO: Element type is Access-Type, long value is 4
3d17h: SSS INFO: Element type is Switch-Id, long value is -1912602284
3d17h: SSS INFO: Element type is Tunnel-Name, string value is server1
3d17h: SSS INFO: Element type is Can-SIP-Redirect, long value is 1

```

```

3d17h: SSS INFO: Element type is AAA-Id, long value is 16729
3d17h: SSS INFO: Element type is AccIe-Hdl, ptr value is 8D00016A
3d17h: SSS MGR [uid:709]: Event service-request, state changed from wait-for-req to
wait-for-auth
3d17h: SSS MGR [uid:709]: Handling Policy Authorize (1 pending sessions)
3d17h: SSS PM [uid:709]: RM/VPDN disabled: RM/VPDN author not needed
3d17h: SSS PM [uid:709]: Multihop disabled: AAA author not needed
3d17h: SSS PM [uid:709]: Multihop disabled: SGF author not needed
3d17h: SSS PM [uid:709]: No more authorization methods left to try, providing default
service
3d17h: SSS PM [uid:709]: Received Service Request
3d17h: SSS PM [uid:709]: Event <found>, State: initial-req to end
3d17h: SSS PM [uid:709]: Handling Service Direction
3d17h: SSS PM [uid:709]: Policy reply - Local terminate
3d17h: SSS MGR [uid:709]: Got reply Local-Term from PM
3d17h: SSS MGR [uid:709]: Event policy-connect local, state changed from
wait-for-auth to connected
3d17h: SSS MGR [uid:709]: Handling Send-Client-Local-Term event
3d17h: VPDN SSS [uid:709]: Event connect local, state changed from SSS to PPP
3d17h: ppp709 PPP: Phase is ESTABLISHING
3d17h: ppp709 LCP: I FORCED rcvd CONFACK len 15
3d17h: ppp709 LCP: MRU 1492 (0x010405D4)
3d17h: ppp709 LCP: AuthProto CHAP (0x0305C22305)
3d17h: ppp709 LCP: MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
3d17h: ppp709 LCP: I FORCED sent CONFACK len 10
3d17h: ppp709 LCP: MRU 1492 (0x010405D4)
3d17h: ppp709 LCP: MagicNumber 0x002AA481 (0x0506002AA481)
3d17h: ppp709 PPP: Phase is FORWARDING, Attempting Forward
3d17h: VPDN SSS [uid:709]: Event dyn bind resp, state changed from PPP to PPP
3d17h: ppp709 PPP: Phase is AUTHENTICATING, Unauthenticated User
3d17h: ppp709 CHAP: O FAILURE id 1 len 25 msg is "Authentication failed"
3d17h: ppp709 PPP: Sending Acct Event[Down] id[4159]
3d17h: ppp709 PPP: Phase is TERMINATING
3d17h: ppp709 LCP: O TERMREQ [Open] id 1 len 4
3d17h: ppp709 LCP: State is Closed
3d17h: ppp709 PPP: Phase is DOWN
3d17h: ppp709 PPP: Phase is TERMINATING
3d17h: VPDN SSS [uid:709]: Event peer disc, state changed from PPP to DSC
3d17h: nobody@xyz.com Tnl/Sn9349/13589 L2TP: disconnect (AAA) IETF:
17/user-error Ascend: 26/PPP CHAP Fail
3d17h: nobody@xyz.com Tnl/Sn9349/13589 L2TP: O CDN to server1 31399/10
3d17h: Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h: nobody@xyz.com Tnl/Sn9349/13589 L2TP: Destroying session
3d17h: nobody@xyz.com Tnl/Sn9349/13589 L2TP: Session state change from
wait-for-service-selection to idle
3d17h: VPDN SSS [uid:709]: Event vpdn disc, state changed from DSC to END
3d17h: Tnl9349 L2TP: Tunnel state change from established to no-sessions-left
3d17h: Tnl9349 L2TP: No more sessions in tunnel, shutdown (likely) in 10 seconds
3d17h: SSS MGR [uid:709]: Processing a client disconnect
3d17h: SSS MGR [uid:709]: Event client-disconnect, state changed from connected to
end
3d17h: SSS MGR [uid:709]: Handling Send-Service-Disconnect event
3d17h: Tnl9349 L2TP: O StopCCN to server1 tnid 31399
3d17h: Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h: Tnl9349 L2TP: Tunnel state change from no-sessions-left to shutting-down
3d17h: Tnl9349 L2TP: Shutdown tunnel

```

Additional References

For additional information related to Subscriber Service Switch, refer to the following references:

Related Documents

Related Topic	Document Title
“Virtual Templates, Profiles, and Networks” chapter “PPP Configuration” chapter	<ul style="list-style-type: none"> • Cisco IOS Dial Technologies Configuration Guide, Release 12.2
VPDN and PPP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<ul style="list-style-type: none"> • Cisco IOS Dial Technologies Command Reference, Release 12.2
“Authentication, Authorization, and Accounting (AAA)” chapter	<ul style="list-style-type: none"> • Cisco IOS Security Configuration Guide, Release 12.2
AAA commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<ul style="list-style-type: none"> • Cisco IOS Security Command Reference, Release 12.2
“Configuring Broadband Access: PPP and Routed Bridging Encapsulations” chapter	<ul style="list-style-type: none"> • Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2
PPPoE and PPPoA commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<ul style="list-style-type: none"> • Cisco IOS Wide-Area Networking Command Reference, Release 12.2
L2TP tunnel service authorization	<ul style="list-style-type: none"> • L2TP Tunnel Service Authorization Enhancements
LLID feature	<ul style="list-style-type: none"> • RADIUS Logical Line ID

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
RFC 2341	<i>Cisco Layer Two Forwarding (Protocol) L2F</i>
RFC2661	<i>Layer Two Tunneling Protocol L2TP</i>
RFC 2516	<i>A Method for Transmitting PPP Over Ethernet (PPPoE) (PPPoE Discovery)</i>

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and 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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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 <i>type number</i>	Interface keyword followed by the interface type and number.
vc [<i>vpi</i>]/ <i>vci</i>	(Optional) Virtual circuit (VC) keyword followed by a virtual path identifier (VPI), virtual channel identifier (VCI). A slash (/) follows the VPI.
<i>vc-name</i>	(Optional) Name of the VC.
vlan <i>vlan-id</i>	(Optional) VLAN identifier.
rmac <i>mac-address</i>	(Optional) Remote MAC address.
sid <i>session-id</i>	(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 <i>vlan-id</i> keyword and argument were added.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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*]*vci* | *virtual-circuit-name*}

Syntax Description	event	PPPoA events.
	error	PPPoA errors.
	state	PPPoA state.
	interface atm <i>interface-number</i> [<i>subinterface-number</i>]	(Optional) Specifies a particular ATM interface by interface number and optionally a subinterface number separated by a period.
	vc [<i>vpi/vci</i>] <i>vci</i> <i>virtual-circuit-name</i>	(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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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 3 *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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Examples The following example shows how to enter this command. See the “Examples” section of the [debug ssg transparent login](#) 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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Examples

The following example shows how to enter this command. See the “Examples” section of the **debug ssg transparent login** 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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Examples

The following example shows how to enter this command. See the “Examples” section of the [debug ssg transparent login](#) 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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Examples

The following example shows how to enter this command. See the “Examples” section of the [debug ssg transparent login](#) command page for an example of output.

```
Router# debug sss fsm
```


multihop hostname

To enable the Layer 2 Tunnel Protocol (L2TP) tunnel switch to initiate a tunnel based on the L2TP access concentrator (LAC) host name or ingress tunnel ID, use the **multihop hostname** command in VPDN request-dialin group 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 LAC hostname or ingress tunnel ID.

Defaults

No default behavior or values.

Command Modes

VPDN request-dialin group 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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Examples

The following example enables the L2TP tunnel switch to forward sessions from LAC-1 through an outgoing tunnel to IP address 10.3.3.3 using a virtual private dialup network (VPDN) group:

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

show pppatm summary

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

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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 example that follows. 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 VA/SID	VCI State	Conn ID	PPPoA ID	SSS ID	PPP ID	AAA ID	VT
6	101	11	DA000009	BB000013	E5000017	C	1
1.1	PTA						

Most of the messages displayed by the **show pppatm summary** command are self-explanatory. [Table 4](#) describes the significant fields shown in the displays. Any data not described in [Table 4](#) is used for internal debugging purposes.

Table 4 *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 <i>interface-number</i>	Specifies a particular ATM interface by interface number.
	<i>.subinterface-number</i>	(Optional) Specifies a subinterface number preceded by a period.
	vc [<i>vpi</i>]/ <i>vci</i>	Virtual circuit (VC) keyword followed by a virtual path identifier (VPI), virtual channel identifier (VCI).. The absence of the “/” and a <i>vpi</i> value causes the <i>vpi</i> value to default to 0.
	<i>virtual-circuit-name</i>	Name of the VC.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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@<domain>.com	00:02:36
10	PPPoE/PPP	connected	VPDN	nobody3@<domain>.com	00:01:52
11	PPPoE/PPP	connected	VPDN	nobody3@<domain>.com	00:01:52
3	PPPoE/PPP	connected	VPDN	user3@<domain>.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@<domain>.com	00:02:36
2	PPP	connected	Local Term	user	00:05:06
4	PPP	connected	VPDN	nobody2@<domain>.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@<domain>.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@<domain>.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@<domain>.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@<domain>.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@<domain>.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 user
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@<domain>.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 messages displayed by the **show sss session** and **show sss session all** commands are self-explanatory. [Table 5](#) describes the significant fields shown in the displays. Any data not described in [Table 5](#) is used for internal debugging purposes.

Table 5 *show sss session Field Descriptions*

Field	Description
Unique ID (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: <ul style="list-style-type: none"> 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 (Last Changed)	Time interval in in hh:mm:dd 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 Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F) protocol, and PPP over Ethernet (PPPoE) tunnels in a virtual private dialup network (VPDN), use the **show vpdn session** command in privileged EXEC mode.

show vpdn session [**all** | **packets** | **sequence** | **state**]

Syntax Description

all	(Optional) Combines all keywords and displays extensive reports about the active calls (sessions).
packets	(Optional) Displays information about packet and byte counts for a session.
sequence	(Optional) Displays sequence information.
state	(Optional) Displays state information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	This command was enhanced with the packets keyword to display PPPoE session information.
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 sessions retrieved from other show commands or debug command traces.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

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.

Examples

The following is sample output from the **show vpdn session** command. It provides reports on call activity for the current 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@xyz.com	est	00:06:00	4
5	692	13695	SSS Circuit	nobody1@xyz.com	est	00:01:43	8
6	693	13695	SSS Circuit	nobody1@xyz.com	est	00:01:43	9

show vpdn session

```

3      690    13695 SSS Circuit   nobody3@xyz.com      est    2d21h    3

```

```

L2F Session Information Total tunnels 1 sessions 2

```

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

```

%No active PPTP tunnels

```

```

PPPoE Session Information Total tunnels 1 sessions 7

```

UID	SID	RemMAC	OIntf	Intf	Session state
3	1	0030.949b.b4a0 0010.7b90.0840	Fa2/0	N/A	CNCT_FWDED
6	2	0030.949b.b4a0 0010.7b90.0840	Fa2/0	Vi1.1 UP	CNCT_PTA
7	3	0030.949b.b4a0 0010.7b90.0840	Fa2/0	Vi1.2 UP	CNCT_PTA
8	4	0030.949b.b4a0 0010.7b90.0840	Fa2/0	N/A	CNCT_FWDED
9	5	0030.949b.b4a0 0010.7b90.0840	Fa2/0	N/A	CNCT_FWDED
10	6	0030.949b.b4a0 0010.7b90.0840	Fa2/0	N/A	CNCT_FWDED
11	7	0030.949b.b4a0 0010.7b90.0840	Fa2/0	N/A	CNCT_FWDED

The following is sample output from the **show vpdn session all** command. It provides extensive reports on call activity for all 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@xyz.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@xyz.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@xyz.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@xyz.com
  Interface Se0/0
    Remote session id is 691, remote tunnel id 58582
    UDP checksums are disabled
    IDB switching enabled
    FS cached header information:
      encaps 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@xyz.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@xyz.com
Interface:
```

■ show vpdn session

```

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 messages displayed by the **show vpdn session** and **show vpdn session all** commands are self-explanatory. [Table 6](#) describes the significant fields shown in the displays. Any fields not described in [Table 6](#) are used for internal debugging purposes.

Table 6 *show vpdn session Field Descriptions*

Field	Description
LocID	Local identifier.
RemID	Remote identifier.
CLID	A number uniquely identifying the L2F session.
MID	A number uniquely identifying this user in this tunnel.
TunID	Tunnel identifier.
Intf (Interface:)	Virtual access interface associated with the session.
Username (User:)	User domain name.
State (State:)	<p>Status for the individual user in the tunnel; can be one of the following states:</p> <ul style="list-style-type: none"> • est • opening • open • closing • closed • waiting_for_tunnel <p>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.</p>

Table 6 *show vpdn session Field Descriptions (continued)*

Field	Description
Last Chg	Time interval (in hh:mm:ss) since last change occurred.
Uniq ID (Unique ID:)	The unique identifier used to correlate this particular session with the sessions retrieved from other show commands or debug command traces.
UID	PPPoE user ID.
SID	PPPoE session ID.
RemMAC	Remote Media Access Control (MAC) address of the host.
OIntf	Outgoing interface.
Session	PPPoE session identifier.
Session id	L2TP session identifier.
tunnel id	L2TP tunnel identifier.
Pkts-Out (Packets out:)	Number of packets going out of this session.
Bytes-Out (Bytes out:)	Number of bytes going out of this session.
Pkts-In (Packets in:)	Number of packets coming into this session.
Bytes-In (Bytes in:)	Number of bytes coming into this session.

The following is sample output from the **show vpdn session packets** command for a 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 7](#) describes the significant fields shown in the **show vpdn session packets** command display.

Table 7 *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.

Related Commands	Command	Description
	show sss session	Displays Subscriber Service Switch session status.
	show vpdn tunnel	Displays information about active L2TP, L2F protocol, and PPPoE tunnels in a VPDN.
	vpdn enable	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
	vpdn group	Associates a VPDN group to a customer or VPDN profile.
	vpdn history failure	Enables logging of VPDN failures to the history failure table or to sets the failure history table size.

subscriber access

To configure an L2TP access concentrator (LAC) to enable Subscriber Service Switch (SSS) to preauthorize the network access server (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** [*aaa-method-list*]

no subscriber access { **pppoe** | **pppoa** } **pre-authorize nas-port-id** [*aaa-method-list*]

Syntax Description	pppoe	Specifies PPP over Ethernet (PPPoE).
	pppoa	Specifies PPP over ATM (PPPoA).
	pre-authorize nas-port-id	Signals SSS to preauthorize the NAS-Port-ID string before authorizing the domain name.
	<i>aaa-method-list</i>	(Optional) Authentication, authorization, and accounting (AAA) method list name.

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 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.
	12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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 in 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 AV-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_water
  server 172.20.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization cfg-commands
aaa authorization network default group sg_water
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_water password 0 lab
vpdn enable
!
vpdn-group 2
  request-dialin
  protocol l2tp
  domain <domain>.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
```

Related Commands

Command	Description
subscriber authorization enable	Enables SSS type authorization.
vpdn authorize domain	Enables domain preauthorization on a NAS.

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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

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 preauthorization.
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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

A RADIUS domain preauthorization user profile must also be created. See the “Examples” section and refer to the latest edition of 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  
  }  
}
```

vpn service

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

vpn service *domain-name*

no vpn service *domain-name*

Syntax Description

<i>domain-name</i>	Static domain name.
--------------------	---------------------

Defaults

No default behavior or values

Command Modes

ATM VC configuration
ATM VC class 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(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

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

Examples

In the following partial example, virtual private dialup network (VPDN) group 1 is selected for PPPoA session forwarding based on the domain name domain.com:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain <domain>.com
  initiate-to ip 10.1.1.1 priority 1
.
.
.
interface ATM1/0.1 multipoint
 pvc 101
  protocol ppp virtual-template 1
  vpn service domain.com
```

Glossary

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

L2TP access concentrator—See LAC.

L2TP network server—See LNS.

Layer 2 Forwarding Protocol—See L2F.

Layer 2 Tunneling Protocol—See L2TP.

L2F—Layer 2 Forwarding Protocol, as described in RFC 2341.

L2TP—Layer 2 Tunneling Protocol, as described in RFC2661.

LAC—L2TP access concentrator. The peer of the LNS that serves as one endpoint of an L2TP tunnel. The client connects to the LAC directly and PPP frames are tunneled over L2TP to the LNS.

LLID—logical line identification. An alphanumeric string that is a minimum of one character and a maximum of 253 characters in length, which is the logical identification of a subscriber line. LLID is maintained in a RADIUS server customer profile database. This customer profile database is connected to a LAC and is separate from the RADIUS server that the LAC and LNS use for the authentication and authorization of incoming users. When the customer profile database receives a preauthorization request from the LAC, the server sends the LLID to the LAC as the Calling-Station-ID attribute (attribute 31).

LNS—L2TP network server. A node that acts as one side of an L2TP tunnel endpoint. A peer to the LAC. The logical termination point of a PPP session that is being tunneled by the LAC.

locally terminated—Refers to a PPP session that will no longer be forwarded. The PPP framing and negotiation ends at this point to allow Layer 3 processing of the framed packet.

logical line identification—See LLID.

MLP—Multilink PPP. Method of splitting, recombining, and sequencing datagrams across multiple logical data links.

multihop—Traditional term for accepting a PPP session from a virtual private dial-up network (VPDN) protocol such as L2TP or L2F and tunneling it back out via L2TP or L2F.

Multilink PPP—See MLP.

NAS—network access server, the L2F equivalent of a LAC.

network access server—See NAS.

Packet Data Serving Node—See PDSN.

PDSN—Packet Data Serving Node. Provides access to the Internet, intranets and applications servers for mobile stations utilizing a cdma2000 Radio Access Network (RAN). Acting as an access gateway, PDSN provides simple IP and mobile IP access, foreign agent support, and packet transport for virtual private networking. It acts as a client for authentication, authorization, and accounting (AAA) servers and provides mobile stations with a gateway to the IP network. Mobility differentiates Cisco's PDSN from the traditional routed network. With PDSN, the host can move and, therefore, there must be a way to forward packets to it. Cisco's PDSN solution offers a secure way to provide packet data services to mobile stations.

PPPoA—PPP over ATM.

PPPoE—PPP over Ethernet (RFC 2516). Refers to the signaling protocol defined within PPPoE and as the encapsulation method. Sometimes ambiguous as to whether this term refers to PPPoE over ATM or PPPoE directly over Ethernet.

PPPoEoA—PPP over Ethernet over ATM. The most common form of PPPoE into LAC.

PPPoEoE—This acronym is often used to differentiate actual PPP over Ethernet from PPPoEoA, but does not imply that PPP is being encapsulated in two levels of Ethernet.

PPPoX—Either PPPoEoA, PPPoEoE, or PPPoA.

service—What a subscriber is provided. Example of a service may be tunneling an incoming PPP session from PPPoE to another location via L2TP, or local termination of the PPPoE session. In addition, QoS parameters or other specifics may be bundled as part of an identified service.

service key—An elemental piece of information about a subscriber that is used to determine a service for that subscriber. Examples include the PPP authenticated name, ATM VPI/VCI, the PPPoE service name, and so on.

SGF—stack group forwarding. Process used by the Stack Group Bidding Protocol (SGBP) to authorize a session for forwarding.

stack group forwarding—See SGF.

subscriber—An access user that typically uses a PPP-based service. This service may be PPPoE, PPPoA, L2TP, PPP over a dial infrastructure such as ISDN or analog, and so on.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2002, 2005 Cisco Systems, Inc. All rights reserved.

