



Junos[®] OS

ANCP Agent Feature Guide for Subscriber Management

Release

14.1



Published: 2014-04-25

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos[®] OS ANCP Agent Feature Guide for Subscriber Management

14.1

Copyright © 2014, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xv
	Opening a Case with JTAC	xvi
Part 1	Overview	
Chapter 1	ANCP in Subscriber Access Networks	3
	ANCP and the ANCP Agent Overview	3
	Overview	3
	Topology Discovery	4
	Subscriber Services	4
	ANCP Interfaces and Access Loop Circuit Identifiers	5
	ANCP Neighbors	6
	Partitions	8
	Generic Response Messages and Result Codes	8
	Traffic Rate Reporting and Adjustment by the ANCP Agent	10
	Overview	10
	Traffic Rate Adjustment	11
	Recommended Traffic Shaping Rates	12
	ANCP Agent Keepalives for CoS	12
	ANCP Agent Interactions with AAA	13
	ANCP Operations in Different Network Configurations	15
	ANCP Network Using N:1 and 1:1 Configuration Models without Interface Sets	18
	Sequence of ANCP Events: Static VLAN or VLAN Demux Interfaces over Ethernet Without Interface Sets	19
	ANCP Network Using N:1 Configuration Model with Interface Sets	20
	Sequence of ANCP Events: Static VLAN Interfaces over Ethernet with Interface Sets	21
	ANCP Network Using 1:1 Configuration Model with Interface Sets	22

	Sequence of ANCP Events: Static VLAN Demux Interfaces over Aggregated Ethernet with Interface Sets	23
	ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes	23
	Preservation of CoS Shaping Across ANCP Agent Restarts	25
Part 2	Configuration	
Chapter 2	Configuration Overview	29
	Configuring the ANCP Agent	29
Chapter 3	Configuration Tasks for ANCP	31
	Configuring ANCP Neighbors	31
	Associating an Access Node with Subscribers for ANCP Agent Operations	32
	Specifying the Interval Between ANCP Adjacency Messages	33
	Specifying the Maximum Number of Discovery Table Entries	34
	Configuring the ANCP Agent for Backward Compatibility	34
	Specifying How Long Processes Wait for the ANCP Agent Restart to Complete	35
	Configuring the ANCP Agent to Learn ANCP Partition IDs	35
	Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates	36
	Configuring the ANCP Agent to Report Traffic Rates to CoS	37
	Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces	38
	Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages . .	40
	Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications	41
	Triggering ANCP OAM to Test the Local Loop	41
Chapter 4	Example	43
	Example: Configuring an ANCP Network with Interface Sets and N:1 Static Demux VLANs over Aggregated Ethernet	43
Chapter 5	Configuration Statements	65
	[edit protocols ancp] Hierarchy Level	66
	access-identifier	67
	adjacency-timer	68
	advisory-options (Traffic Shaping)	69
	ancp	70
	ancp-speed-change-immediate-update (ANCP)	71
	downstream-rate (Traffic Shaping)	72
	exclude (RADIUS)	73
	gsmp-syn-timeout (ANCP)	77
	gsmp-syn-wait (ANCP)	78
	ietf-mode	78
	interface-set (ANCP)	79
	interfaces (ANCP)	80
	juniper-dsl-attributes	81
	maximum-discovery-table-entries	82
	maximum-helper-restart-time	82

	neighbor (Define ANCP)	83
	overhead-accounting (ANCP)	84
	pre-ietf-mode	85
	qos-adjust	85
	qos-adjust-adsl	86
	qos-adjust-adsl2	86
	qos-adjust-adsl2-plus	87
	qos-adjust-sdsl	87
	qos-adjust-vdsl	88
	qos-adjust-vdsl2	88
	traceoptions (ANCP)	89
	underlying-interface (ANCP)	91
	upstream-rate (Traffic Shaping)	92
Part 3	Administration	
Chapter 6	Monitoring ANCP for Subscriber Access	95
	Verifying and Monitoring ANCP Neighbors	95
	Clearing ANCP Neighbors	96
	Verifying and Monitoring ANCP Subscribers	96
	Clearing ANCP Subscribers	97
	Verifying and Monitoring CoS for ANCP Subscribers	97
	Clearing and Verifying ANCP Statistics	97
Chapter 7	Monitoring Commands	99
	clear ancp neighbor	100
	clear ancp statistics	102
	clear ancp subscriber	104
	request ancp oam interface	106
	request ancp oam neighbor	107
	show ancp cos	108
	show ancp neighbor	111
	show ancp statistics	119
	show ancp subscriber	124
	show ancp summary	129
	show ancp summary neighbor	131
	show ancp summary subscriber	133
Part 4	Troubleshooting	
Chapter 8	Acquiring Troubleshooting Information	137
	Tracing ANCP Agent Operations for Subscriber Access	137
	Configuring the ANCP Trace Log Filename	138
	Configuring the Number and Size of ANCP Log Files	138
	Configuring Access to the ANCP Log File	139
	Configuring a Regular Expression for ANCP Messages to Be Logged	139
	Configuring the ANCP Tracing Flags	140
	Configuring the Severity Level to Filter Which ANCP Messages Are Logged	140
	Collecting Subscriber Access Logs Before Contacting Juniper Technical Support	141

Chapter 9	Troubleshooting Configuration Statement	143
	traceoptions (ANCP)	144
Part 5	Index	
	Index	149

List of Figures

Part 1	Overview	
Chapter 1	ANCP in Subscriber Access Networks	3
	Figure 1: Sample ANCP Topology Without Interface Sets (1:1 and N:1 Model)	18
	Figure 2: Sample ANCP Topology with Interface Sets (N:1 Model)	20
	Figure 3: Sample ANCP Topology with Interface Sets (1:1 Model)	22
Part 2	Configuration	
Chapter 4	Example	43
	Figure 4: N:1 ANCP Topology with Interface Sets and VLAN Demux Interface over Aggregated Ethernet	45

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiii
Part 1	Overview	
Chapter 1	ANCP in Subscriber Access Networks	3
	Table 3: ANCP Failure Result Codes	9
	Table 4: ACI Mapping by Interface Type for the ANCP 1:1 Model	16
	Table 5: ACI Mapping by Interface Set Type for the ANCP N:1 Access Model	16
	Table 6: Mapping ANCP DSL Attributes to Juniper Networks DSL VSAs and DSL Forum VSAs	24
Part 2	Configuration	
Chapter 4	Example	43
	Table 7: Configuration Components used in ANCP N:1 Topology Example with Interface Sets	45
Part 3	Administration	
Chapter 7	Monitoring Commands	99
	Table 8: show ancp cos Output Fields	108
	Table 9: show ancp neighbor Output Fields	111
	Table 10: show ancp statistics Output Fields	119
	Table 11: show ancp subscriber Output Fields	124
	Table 12: show ancp summary Output Fields	129
	Table 13: show ancp summary neighbor Output Fields	131
	Table 14: show ancp summary subscriber Output Fields	133

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Using the Examples in This Manual on page xi
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xv

Documentation and Release Notes

To obtain the most current version of all Juniper Networks[®] technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xiii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<pre>user@host> show chassis alarms</pre> <p>No alarms currently active</p>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	<p>Configure the machine's domain name:</p> <pre>[edit] root@# set system domain-name domain-name</pre>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop address; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview

- [ANCP in Subscriber Access Networks on page 3](#)

CHAPTER 1

ANCP in Subscriber Access Networks

- [ANCP and the ANCP Agent Overview on page 3](#)
- [Traffic Rate Reporting and Adjustment by the ANCP Agent on page 10](#)
- [ANCP Agent Interactions with AAA on page 13](#)
- [ANCP Operations in Different Network Configurations on page 15](#)
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 23](#)
- [Preservation of CoS Shaping Across ANCP Agent Restarts on page 25](#)

ANCP and the ANCP Agent Overview

This topic describes the Access Node Control Protocol (ANCP) and the *ANCP agent*. The ANCP agent is the Junos OS process that manages subscriber access lines with ANCP. The agent monitors subscriber access lines, reports subscriber traffic rates on the access lines between the subscribers and the access nodes, and modifies the traffic rates, all in support of CoS traffic shaping.

- [Overview on page 3](#)
- [Topology Discovery on page 4](#)
- [Subscriber Services on page 4](#)
- [ANCP Interfaces and Access Loop Circuit Identifiers on page 5](#)
- [ANCP Neighbors on page 6](#)
- [Partitions on page 8](#)
- [Generic Response Messages and Result Codes on page 8](#)

Overview

ANCP acts as a control plane between a service-oriented Layer 3 edge device and a Layer 2 access node. The access nodes—ANCP *neighbors*—are network devices that terminate access loops from subscribers; for DSL access loops, the access node is a DSL access multiplexer (DSLAM). Queuing and scheduling mechanisms for subscriber traffic must avoid congestion within the access network while contending with multiple flows and distinct CoS requirements. These mechanisms require the edge device—a router acting as a broadband network gateway (BNG), often also called a network access server (NAS)—to provide information about the access network and subscriber traffic.

The ANCP agent can map an access line to an interface or interface set either statically or dynamically. The agent provides that information to both CoS and AAA. The agent passes on to both CoS and AAA the traffic shaping attributes for each subscriber access line that the access node sent to the ANCP agent. In addition, the agent sends to AAA all DSL Forum attributes that were sent by the access node. AAA can use these attributes during RADIUS accounting and authentication for both DHCP IP demux and PPPoE subscriber sessions. The traffic rates can also be used for shaping L2TP tunnel traffic.

You can monitor ANCP agent events and operations by including the **traceoptions** statement at the **[edit protocols ancp]** hierarchy level.

Junos OS supports the following interface types for ANCP:

- Static VLAN interfaces
- Static VLAN demux interfaces
- Static interface sets
- Dynamic interface sets
- Dynamic VLAN-tagged interface sets
- Dynamic agent circuit identifier (ACI) interface sets, also known as ACI sets or ACI VLANs
- Dynamic PPPoE and DHCP IP demux subscriber interfaces

ANCP was developed as an extension of *RFC 3292, General Switch Management Protocol (GSMP) V3*, but is now defined in *RFC 6320, Protocol for Access Node Control Mechanism in Broadband Networks*.

Topology Discovery

The router uses topology discovery to collect information from the access node. The information includes the following:

- Topology of the access network
- DSL line state
- Actual upstream and downstream net data rates of a synchronized DSL link
- Maximum attainable upstream and downstream net data rates
- Interleaving delay

Subscriber Services

The router receives the service profile for the subscribers from a RADIUS server. Most of the services are enforced by the router itself. The router shapes the aggregate egress traffic to subscribers based on the local loop throughput reported by the DSLAM. This traffic shaping optimizes traffic flow while avoiding traffic drops in the access node.

Some service attributes, such as interleaving delay and multicast channel information, are enforced at the access node. The ANCP agent provides the line configuration

mechanism that the edge device can use to pass the line configuration to the access nodes. Typically, multiple profiles are provisioned on the access node. The router instructs the access node which profile to use for a given subscriber.

Subscribers typically receive some combination of voice, data, and video services. Each service can be provisioned on a VLAN. A subscriber might receive only a single service over a single VLAN configured on a logical interface. A group of VLANs carrying services to a subscriber is an *interface set*.

Subscribers have operational states, but they do not have administrative states because they cannot be configured in the CLI.

Subscribers have one of the following operational states which represent the DSL line state as it is reported in the ANCP Port Up and Port Down messages sent by an access node:

- Idle—Ports are not configured and the subscriber cannot log in.
- Silent—Ports are configured and the subscriber is connected, but the DSL modem is not ready to transfer data.
- Showtime—Ports are configured, the subscriber is connected, and the DSL modem is online and ready to transfer data.

ANCP Interfaces and Access Loop Circuit Identifiers

The access loop or access line in an ANCP topology consists of the physical elements between the subscriber device (CPE) and the access node. An identifier associated with the access loop serves to identify the subscriber as well. This identifier is an alphanumeric string that actually identifies the interface on the DSLAM from which subscriber requests originate. It can be referred to by various names.

- In ANCP messages, a TLV carries the access loop circuit ID, also referred to as the access line identifier, access loop circuit identifier, or access identifier.
- DHCP discovery packets can identify the line with the Agent Circuit ID suboption in the Option 82 field.
- PPPoE discovery packets can identify the line with the Agent-Circuit-ID subattribute in the DSL Forum vendor-specific tag.

Each of these identifiers is abbreviated as ACI. When the ANCP agent receives a port management message from an access node, it uses the access loop circuit identifier contained in the message to determine which logical interface or interface set corresponds to the subscriber.

You can associate an identifier with an ANCP access line by static configuration. When you configure a logical interface by specifying the interface name at the **[edit protocols ancp interfaces]** hierarchy level, include the **access-identifier** statement to associate the access loop circuit identifier with the interface. When you configure an interface set by including the **interface-set** statement at the **[edit protocols ancp interfaces]** hierarchy level, associate the access loop circuit identifier with the interface set by including the

access-identifier statement at the **[edit protocols ancp interfaces interface-set interface-set-name]** hierarchy level.

When the DHCP or PPPoE discovery packet includes an ACI, the ANCP agent can dynamically map the ACI to the subscriber interface or interface set. VLANs for the subscribers are created according to a dynamic profile; these are called agent circuit identifier-based or ACI-based dynamic VLANs.

ANCP agent support for RADIUS authentication and accounting requires that both static and dynamic ACIs must be unique across the network. No two interfaces across multiple neighbors (access nodes) can share the same identifier. The DHCP and PPPoE processes do not have information about the access node IP addresses and consequently cannot distinguish between duplicate identifiers. This situation prevents the AAA services framework from correlating a DHCP or PPPoE client session with an access line for RADIUS authentication and accounting.

ANCP Neighbors

The ANCP agent can report traffic only for access nodes that are configured as ANCP neighbors (also referred to as ANCP peers). Neighbors can establish TCP connections with the router. Include the **neighbor** statement at the **[edit protocols ancp]** hierarchy level to configure an access node as an ANCP neighbor.

The ANCP agent exchanges adjacency messages with neighbors. If an adjacency message is not received from a neighbor within the expected period, then the neighbor is considered to be down and is disconnected. You can adjust how long the ANCP agent waits for adjacency messages from all neighbors by including the **adjacency-timer** statement at the **[edit protocols ancp]** hierarchy level. The interval between adjacency messages is negotiated between router and the neighbor during adjacency establishment. The larger of two timer values—either the value received in the ANCP SYN message or the configured value—is selected. Loss of synchronization between the router and a neighbor is declared when no valid messages are received for a period of time that exceeds three times the negotiated value.



NOTE:

The ANCP TCP connection is not established and consequently ANCP neighbors do not come up in either of the following circumstances:

- When the neighbor address (numbered or unnumbered) has a /32 mask.
- When the unnumbered local address for ANCP dynamic logical interfaces is configured to use a preferred source address.

ANCP neighbors have one of the following administrative states, which simply represent the configuration of the neighbor:

- enabled—The neighbor is configured in the CLI.
- disabled—The neighbor is not configured, meaning either that it has never been configured or that the configuration has been deleted.

ANCP neighbors in the enabled state have one of the following operational states, which represent the state of adjacency negotiations:

- **Configured**—The neighbor has been configured, but has never established an adjacency.
- **Establishing**—Adjacency negotiations are in progress.
- **Established**—Adjacency negotiations have succeeded and an ANCP session has been established.
- **Not Established**—The neighbor has lost a previously established adjacency, but is ready to begin negotiations.

You can also configure parameters for a specific neighbor that override global or default configurations by including any of the following statements at the **[edit protocols ancp neighbor ip-address]** hierarchy level:

- **adjacency-timer**—Adjust the interval between adjacency messages exchanged with this neighbor.
- **ietf-mode**—Prevent the ANCP agent from operating in a backward-compatible mode for this neighbor; for neighbors that use the current IETF implementation of ANCP.
- **maximum-discovery-table-entries**—Specify how many discovery table entries are accepted from this neighbor. Include this statement at the **[edit protocols ancp]** hierarchy level to set the number of entries globally for all neighbors.
- **pre-ietf-mode**—Enable the ANCP agent to operate in a backward-compatible mode for this neighbor; for neighbors that use the original IETF implementation of ANCP (GSMPv2) rather than the current implementation. Include this statement at the **[edit protocols ancp]** hierarchy level to operate in backward-compatible mode globally for all neighbors.

RFC 6320, Protocol for Access Node Control Mechanism in Broadband Networks, defines ANCP Version 1. ANCP was originally implemented based on General Switch Management Protocol (GSMP) version 3, sub-version 1. However, the Internet community has made so many extensions and modifications to GSMPv3 in the course of developing ANCP that ANCP is no longer interoperable with GSMPv3. Consequently, ANCP neighbors must be able to dynamically detect the version that each peer supports. A joint registry codifies the GSMP and ANCP version numbers.

When an ANCP neighbor opens adjacency negotiations, it indicates the highest version of ANCP that it supports, either 0x31 for GSMPv3 or 0x32 for ANCP Version 1. (Version 1 may also be called Version 50, referring to the decimal conversion from the hexadecimal value.) If the receiving neighbor supports that version of ANCP, it returns that value when it responds to the sending neighbors. If it does not support that version, the receiving neighbor simply drops the message.

The ANCP agent stores information about active ANCP subscribers in the Junos shared database, including DSL attributes for the access lines. This storage is persistent and is removed from the database only when one of the following commands is issued:

-

The persistence of the storage enables PPPoE and DHCP IP demux subscribers to be properly managed by RADIUS for authentication and accounting, with their DSL attributes, even when the ANCP connection has been temporarily terminated.

Partitions

ANCP supports the division of an access node into logical partitions. Each partition creates an adjacency with a router; each partition on an access node can form adjacencies with different routers.

Each partition has an identifier carried in ANCP messages. A partition type field in ANCP messages indicates whether the access node is partitioned and how the partition identifier is negotiated. The field has one of the following values negotiated during the formation of the adjacency:

- 0—The access node is not partitioned or does not support partitions.
- 1—The number of partitions is fixed and the router requests the access node to use the identifier it places in the partition identifier field.
- 2—The number of partitions is fixed and the access node has assigned the partition identifier.

ANCP messages include a partition ID field that indicates one of the following scenarios for ANCP agent support of the neighbor:

- Zero partition ID—The ANCP agent supports each neighbor on an IP address over a single TCP session with a partition ID of zero. This is the default support case.
- Single nonzero partition ID—The ANCP agent supports each neighbor on an IP address over a single TCP session with a nonzero partition ID. This case requires partition ID learning to be enabled with the **gsmp-syn-wait** statement at the **[edit protocols ancp]** hierarchy level.

Generic Response Messages and Result Codes

ANCP neighbors and the router can reply to messages either with a specific response message or a generic response message. A generic response message is typically sent when no information needs to be sent to the peer other than a success or failure result. If the response is about a failure, then a result code is included that specifies the kind of failure; a limited amount of diagnostic data can also be included. A generic response message can also be sent independently of a request if the adjacency is being shut down because of the failure. In this case, the sender of the message zeros out the Transaction ID field in the message header and the Message Type field in the Status-Info TLV.

[Table 3 on page 9](#) describes the result codes that can be included in a generic response message.

Table 3: ANCP Failure Result Codes

Code Value	Description	Detected By
0x02	Although the request message is properly formed, it is invalid because it violates the protocol, either because of timing issues such as a race condition or the direction in which the message was transmitted.	ANCP agent
0x06	One or more of the specified ports is down because of a state mismatch between the router and an ANCP control application.	Control applications (none yet available)
0x13	ANCP is out of resources. This result code is sent only by the access node; the problem is probably not related to the access lines, but can be related to a specific request.	ANCP protocol layer or control applications (none yet available)
0x51	The type of request message is not implemented because of a mismatch in protocol versions or capability state between the peers, or possibly because the message type is optional for an ANCP capability.	ANCP agent
0x53	The message is malformed either because it was corrupted in transit or an implementation error occurred at one end of the connection.	ANCP agent
0x54	One or more mandatory TLVs is missing from the request.	ANCP agent
0x55	The contents of one or more TLVs in the request are invalid because they do not match the TLV specification.	ANCP agent
0x500	One or more of the ports specified in a request does not exist, possibly because of a configuration mismatch between the access node and the router or AAA.	Control applications (none yet available)



NOTE: Although Junos OS supports both sending and receiving generic response messages, currently the ANCP agent only receives these messages. When one of these messages is received, the router generates a system log, increments the generic message counters, and increments the result code counters. When the ANCP agent receives an incorrect or unexpected generic response message from an ANCP neighbor, it immediately drops the packet, generates a system log notice message, and takes no further action.

Generic response messages usually include the Status-Info TLV, which includes supplemental information about a warning or error condition. The Status-Info TLV is required when the result code indicates any of the following: a port is down or does not exist, a mandatory TLV is missing, or a TLV is invalid. The Status-Info TLV can also be included in other ANCP message types.

**Related
Documentation**

- [Traffic Rate Reporting and Adjustment by the ANCP Agent on page 10](#)
- [Configuring the ANCP Agent on page 29](#)
- [Triggering ANCP OAM to Test the Local Loop on page 41](#)
- [Agent Circuit Identifier-Based Dynamic VLANs Overview](#)

Traffic Rate Reporting and Adjustment by the ANCP Agent

The ANCP agent monitors the subscriber access lines and reports to AAA and CoS information about the lines that it receives from the access node.

- [Overview on page 10](#)
- [Traffic Rate Adjustment on page 11](#)
- [Recommended Traffic Shaping Rates on page 12](#)
- [ANCP Agent Keepalives for CoS on page 12](#)

Overview

The ANCP agent reports two kinds of data rates:

- The *net data rate* is the portion of the total data rate that can be used to transmit user information. The net data rate is also called the *unadjusted* traffic rate.
- However, each DSL line type has a certain technology overhead; so the actual rate for user data is less than the net data rate. The *adjusted* or *calculated* rate is the net data rate reduced by the amount of technology overhead incurred by each DSL line type. The result is a closer approximation of the actual rate of subscriber data traffic. You can configure the ANCP agent to adjust the net data rate by a fixed percentage for each line type to generate the adjusted rate.

The ANCP agent reports traffic rates differently to AAA and CoS.

- The agent always reports both unadjusted and adjusted rates for both upstream and downstream traffic to AAA in response to a AAA request.
- The agent always reports only unadjusted downstream traffic rates to CoS in support of CoS traffic shaping. It never reports upstream traffic rates to CoS because CoS does not shape upstream traffic. It never reports adjusted traffic rates to CoS. In addition to the unadjusted downstream rate, the agent also reports to CoS the overhead mode and bytes for the access line; CoS can use this information when it subsequently shapes the traffic.

When you remove a shaping rate configuration that the ANCP agent previously applied, the traffic shaping rate reverts to the CoS session shaping as determined by the CoS

traffic-control profiles specified in the dynamic profile. If the ANCP agent remains running but loses a connection to a particular neighbor whose subscriber traffic has been adjusted as a result of ANCP agent action, the adjusted rate remains in effect. The rate currently in effect changes only when the ANCP agent restores the connection and sends fresh updates to CoS, or when you remove the **qos-adjust** statement.

Because CoS can perform traffic shaping only when a traffic-control profile has been applied to the interface or interface set, the expectation might be that traffic shaping is always influenced by the ANCP agent when the ANCP subscriber interface or interface set has a traffic-control profile. However, this is not always true.

Consider a configuration where a subscriber logical interface is a member of an ACI-based VLAN (interface set) and therefore they share the same ACI. The dynamic profile that instantiates the subscriber interface applies a traffic-control profile to the interface. The profile that instantiates the VLAN applies an interface-shared filter instead of a traffic-control profile.

When the subscriber logs in, the first packet creates the auto-sensed, underlying VLAN. The second packet creates the ACI-based subscriber VLAN. The third packet creates the subscriber logical interface. Because the VLAN comes up first, the ANCP agent attaches to the VLAN and not to the interface.

The agent therefore reports to CoS the downstream data rate only for the VLAN, not for the logical interface. Thus CoS has no information to adjust the shaping rate for the interface, and can only shape traffic for the interface only according to the interface's traffic-control profile.

Although the agent does report the downstream rate for the VLAN, CoS cannot use that information to shape the VLAN traffic, because the VLAN does not have a traffic-control profile. Consequently, the logical interface's rate cannot be affected by the VLAN rate even though the logical interface is a member of that interface set.

Traffic Rate Adjustment

When a DSLAM determines the data rate on the subscriber local loop, it ignores the additional headers on the DSL line that are associated with the overhead of the access mode (ATM or Ethernet) and the technology of the DSL line type. However, when the ANCP agent subsequently reports a net data rate, by default it includes this overhead and therefore reports a slightly higher value than the actual subscriber data rate seen by the DSLAM.

You can configure the ANCP agent to dynamically adjust the net data rate by a fixed percentage to account for the traffic overhead. To do so, include one or more of the **qos-adjust-dsl-line-type** statements at the **[edit protocols ancp]** hierarchy level. Each of these statements sets an adjustment factor for a particular DSL line type such as ADSL or VDSL2. The adjustment factor is a percentage value that the ANCP agent applies to the traffic rates it receives from the DSLAM. The percentage accounts for the traffic overhead for that line type. That is, you configure the statements for all relevant line types, and the ANCP agent applies the appropriate adjustment when it identifies the line type for the interface. The adjustment factor applies globally for all subscribers of the particular DSL line type associated with the statement: ADSL, ADSL2, ADSL+, SDSL,

VDS1, or VDS2. The ANCP agent subsequently reports the adjusted rate to AAA in addition to the unadjusted data rate.

The **qos-adjust-dsl-line-type** statements are enabled by default with an adjustment factor of 100 percent, meaning that by default the ANCP agent effectively makes no adjustment to the rates.

The ANCP agent reports traffic rates to CoS only when you have included the **qos-adjust** statement at the **[edit protocols ancp]** hierarchy level. However, the ANCP agent only reports net data rates to CoS; it never reports adjusted data rates to CoS. CoS attempts to avoid traffic drops in the access node by itself adjusting the traffic shaping rate that it applies to downstream traffic for a particular VLAN or set of VLANs. The discrepancy between the actual user data rate and the agent-reported net data rate reduces the accuracy of CoS traffic shaping.

Recommended Traffic Shaping Rates

To handle a situation where the router does not receive information from the access node about the downstream and upstream calculated traffic rates for an interface, you can specify recommended *advisory* values for shaping the traffic sent to the interface so that it matches the subscriber local loop speed.

The transmit speed is the recommended traffic value in bits per second used for downstream traffic for an ANCP interface, and is conveyed in the Juniper Networks VSA, Downstream-Calculated-Qos-Rate (IANA 4874, 26–141). The receive speed is the recommended traffic value in bits per second used for upstream traffic for an ANCP interface, and is conveyed in the Juniper Networks VSA, Upstream-Calculated-Qos-Rate VSA (IANA 4874, 26–142).

To set the recommended shaping rates that are used as the default values for these VSAs in static configurations, include the **downstream-rate** and **upstream-rate** statements at the **[edit interfaces interface-name unit logical-unit-number advisory-options]** hierarchy level.

To configure the recommended rates on dynamically created VLAN interfaces, include the **upstream-rate** or **downstream-rate** statements at the **[edit dynamic-profiles profile-name interfaces \$junos-interface-ifd-name unit \$junos-interface-unit advisory-options]** hierarchy level.

To configure the recommended rates on dynamically created ACI interface sets, include the **upstream-rate** or **downstream-rate** statements at the **[edit dynamic-profiles profile-name interface-set \$junos-interface-set-name interfaces \$junos-interface-ifd-name advisory-options]** hierarchy level.

ANCP Agent Keepalives for CoS

The ANCP agent sends a keepalive message to CoS at specific intervals. If CoS does not receive a keepalive in the expected time, it reverts the shaping rate changes it made in response to the ANCP agent. You can adjust how long CoS waits for a keepalive message by including the **maximum-helper-restart-time** statement at the **[edit protocols ancp]** hierarchy level. The interval between keepalive messages is automatically set to one-third the value of the maximum helper restart time. For example, if you set the maximum

helper restart time to 120 seconds, then the ANCP agent sends keepalive messages every 40 seconds. In this example, if CoS does not receive a keepalive message within 120 seconds, then it reverts any policy changes derived from the ANCP agent.

Related Documentation

- [ANCP and the ANCP Agent Overview on page 3](#)
- [Configuring the ANCP Agent on page 29](#)
- [Shaping Rate Adjustments for Subscriber Local Loops Overview](#)
- [Guidelines for Configuring Shaping-Rate Adjustments for Subscriber Local Loops](#)
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 23](#)
- [Preservation of CoS Shaping Across ANCP Agent Restarts on page 25](#)

ANCP Agent Interactions with AAA

The ANCP agent reports both unadjusted (net) data rates and adjusted data rates for subscriber traffic to AAA for RADIUS authentication and accounting of subscriber sessions. The adjusted data rate enables RADIUS to allocate the appropriate services (including class of service) to PPPoE sessions during authentication. The rate reports also enable RADIUS accounting to track the class of service actually provided for the PPPoE sessions, which in turn enables accurate billing for subscriber services.

The access nodes send ANCP DSL attributes in ANCP messages to the router, where they are stored in the shared database. AAA maps the ANCP DSL attributes to both the Juniper Networks DSL VSAs (used by RADIUS) and the DSL Forum VSA subattributes (also called the DSL Forum VSAs). RADIUS uses these attributes during authentication and accounting for PPPoE sessions on the subscriber access line. The attributes persist even when the ANCP session to a given node has ended, enabling RADIUS to later apply these attributes to new sessions on that subscriber access line. To remove the attributes, you must delete the interface or interface set for the access line from the ANCP agent configuration.

The RADIUS profile must be configured to include the **juniper-dsl-attributes** option, or AAA does not report the attributes to RADIUS. If the ANCP DSL attributes are unavailable, AAA maps the session's advisory upstream and downstream data rates (as configured on the session's underlying interface) to the Juniper Networks VSAs, Upstream-Calculated-Qos-Rate [26-142] and Downstream-Calculated-Qos-Rate [26-141], respectively. AAA subsequently provides only these VSAs to RADIUS.

For successful authentication and accounting by RADIUS, AAA has to correlate PPPoE and DHCP IP demux sessions with their access lines and their associated DSL attributes. Some access nodes provide the ACI in PADI/PADR packets for the PPPoE sessions or in the DHCP discovery packets for DHCP IP demux sessions.

When the ACI is not provided in a 1:1 VLAN model with interface sets, you must associate the underlying interface for the sessions with the identifier and the interface set. If you do not configure this association, then only the advisory traffic rates are provided to

RADIUS. This configuration has no effect when the identifier is provided by the access node.

For the N:1 VLAN model with interface sets, the access node must provide the ACI. If you configure the underlying interface for this model when the access node does not provide the identifier, the subscriber sessions can be incorrectly correlated with access lines.

AAA reports values to RADIUS for the Juniper Networks VSAs 26-141 and 26-142 according to the following scheme:

1. When the PPPoE or DHCP IP demux subscriber session can be correlated with an access line, then the ANCP agent adjusts the downstream and upstream traffic rates reported by the access node according to the ANCP agent CoS configuration. The agent then maps the adjusted rates to Upstream-Calculated-Qos-Rate [26-142] and Downstream-Calculated-Qos-Rate [26-141].
2. If the session cannot be correlated with an access line, but the PPPoE or DHCP discovery packet includes the DSL Forum VSA and the Access-Loop-Encapsulation subattribute includes a value for the AAL5 data link, then the ANCP agent adjusts the Actual-Data-Rate-Downstream and Actual-Data-Rate-Upstream subattributes to account for the ATM 48/53 cell tax. The adjusted rates mapped to Upstream-Calculated-Qos-Rate [26-142] and Downstream-Calculated-Qos-Rate [26-141].
3. If neither of the preceding sets of conditions is satisfied, then the ANCP agent simply maps the recommended downstream and upstream data rates to Upstream-Calculated-Qos-Rate [26-142] and Downstream-Calculated-Qos-Rate [26-141]. The recommended rates are either configured statically for the VLAN or VLAN demux interfaces or are in the dynamic profile that creates the interfaces.

To map an ACI to a static VLAN demux interface, include the **access-identifier *identifier*** statement at the **[edit protocols ancp interfaces demux0.logical-unit-number]** hierarchy level.

To configure advisory upstream and downstream data rates on a static VLAN demux interface, include the **upstream-rate *rate*** or **downstream-rate *rate*** statements at the **[edit interfaces demux0 unit *logical-unit-number*]** hierarchy level.

To configure an underlying interface for the PPPoE sessions in an interface set, include the **underlying-interface *interface-name*** statement at the **[edit protocols ancp interfaces interface-set *interface-set-name*]** hierarchy level.

When an ACI, and therefore a subscriber access line, has been mapped to an interface or interface set, the ACI can be re-mapped to a different interface or set. When this happens, traffic shaping is adjusted accordingly for the interfaces or interface sets involved. This capability is useful for the Business Services model, where a PPPoE session that is initially classified as a residential household can be reclassified as a business subscriber during RADIUS authentication by using a Junos OS ICE AAA framework Op-Script application.

In the Business Services Model, the PPPoE session initially represents a residential household until RADIUS authentication and authorization takes place. The ANCP agent

dynamically maps the household's access line to the appropriate subscriber interface and applies CoS traffic shaping to the interface. During authentication and authorization, the Op-Script application may classify the PPPoE session as a business subscriber rather than a residential subscriber. If this occurs, the application creates multiple static VLANs and groups them into an interface set. Based on the ANCP agent configuration, the application then statically maps the subscriber's access line to this static interface set. This interface set can include only static interfaces.

The ANCP agent reverts CoS traffic shaping from the interface previously used by the subscriber and instead applies the shaping to the interface set. This reversion means that the CoS process applies to the interface the next shaping rate in its adjustment control profile.

**Related
Documentation**

- [ANCP and the ANCP Agent Overview on page 3](#)
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 23](#)
- [Configuring the ANCP Agent on page 29](#)
- [Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 40](#)

ANCP Operations in Different Network Configurations

This topic describes different types of supported network configurations and the sequence of events for ANCP operations in representative sample network topologies.

You can configure the ANCP agent for any of the following interface types:

- Static VLAN interfaces
- Static VLAN demux interfaces
- Static interface sets
- Dynamic interface sets
- Dynamic VLAN-tagged interface sets
- Dynamic agent circuit identifier (ACI) interface sets, also known as ACI sets or ACI VLANs
- Dynamic PPPoE and DHCP IP demux subscriber interfaces

Subscriber sessions are dynamically created as needed for each of the devices in a household. Each household can include multiple CPE devices that access the Internet. In all cases, each household is identified by a unique ACI that is assigned by the access node. Additional identifiers are used in some configurations.

The 1:1 and N:1 configuration models determine how VLANs are correlated with households. A network can include one or both of the models:

- 1:1 model—A household has only one PPPoE or DHCP IP demux subscriber session. One or more such households can exist on a single VLAN or VLAN demux interface. In the case of a single household, either the subscriber interface or its underlying VLAN

or VLAN demux interface can represent the household. In the case of multiple households, the corresponding subscriber interfaces represent the households. In either case, the interface representing a household must be mapped to the ACI for its access line.

[Table 4 on page 16](#) describes the types of interfaces supported for the ANCP 1:1 access model when interface sets are not involved, and whether the PPPoE or DHCP IP demux discovery packets must include the ACI for the subscriber access lines.

Table 4: ACI Mapping by Interface Type for the ANCP 1:1 Model

Interface Type	Description	Presence of ACI in Discovery Packets
Dynamic PPPoE or DHCP IP demux interface	When ACI is present in discovery packets, the ANCP agent maps the ACI to the subscriber interface. The name of the interface is automatically generated and nondeterministic.	Required.
Static VLAN or VLAN demux interface	The name of the interface is statically configured. The ANCP agent configuration must include the access-identifier statement to statically map the ACI to the interface.	Not present.

- N:1 model—A household can have more than one PPPoE or DHCP IP demux subscriber session. The household can have more than one VLAN or VLAN demux interface. In either case, all the interfaces must be grouped into an interface set. The interface set in turn must be mapped to the ACI for the household's access line.

An interface set groups the dynamic PPPoE or DHCP IP demux sessions for a household. The subscribers are placed into interface sets by one several methods.

[Table 5 on page 16](#) describes the types of interface sets supported in the ANCP N:1 access model, how they are created, and how the ACI is mapped to the interface set.

Table 5: ACI Mapping by Interface Set Type for the ANCP N:1 Access Model

Type of Interface Set	Description	Interface Type	Presence of ACI in Discovery Packets
ACI-based VLAN interface sets	<p>When the router receives a DHCP or PPPoE discovery packet that includes an ACI embedded within the DSL Forum vendor-specific tag, it dynamically creates the VLAN and the interface set. The router generates a nondeterministic name for the interface set, such as aci-1003-ge-1/0/0.1073741832.</p> <p>The ANCP agent automatically maps the ACI from the discovery packet to the dynamically created interface set.</p> <p>All DHCP IP demux or PPPoE sessions that have the same ACI are mapped to the same interface set.</p>	Dynamic VLAN and VLAN demux interfaces.	Required.

Table 5: ACI Mapping by Interface Set Type for the ANCP N:1 Access Model (*continued*)

Type of Interface Set	Description	Interface Type	Presence of ACI in Discovery Packets
Dynamic interface sets	<p>A dynamic profile dynamically creates the interface set and places interfaces in the set. The profile can either have the name of the interface set explicitly configured or a variable that represents the interface set name. If a variable is used, then the interface set name is provided by RADIUS when it returns an Access-Accept message for the subscriber.</p> <p>The ANCP agent configuration must include the access-identifier statement to statically map the ACI to the interface set.</p> <p>All DHCP IP demux and PPPoE sessions are mapped to an interface set according to the rules of the dynamic profile.</p>	DHCP IP demux subscriber interfaces, PPPoE subscriber interfaces, or VLAN interfaces.	Irrelevant.
Static interface sets	<p>The interface set and set name are statically configured and include multiple static interfaces.</p> <p>The ANCP agent configuration must include the access-identifier statement to statically map the ACI to the interface set.</p>	Static VLAN and VLAN demux interfaces.	Irrelevant.
VLAN-tagged interface sets	<p>When the router receives a DHCP or PPPoE discovery packet that includes a VLAN ID, it dynamically creates the VLAN and the interface set. The interface set is given a deterministic name consisting of the physical interface name and the VLAN tags, for example, ge-1/0/0-101.</p> <p>The ANCP agent configuration must include the access-identifier statement to statically map the ACI to the interface set.</p> <p>All DHCP IP demux or PPPoE sessions that have the same VLAN ID tag are mapped to the same interface set.</p>	Dynamic VLAN and VLAN demux interfaces.	Irrelevant.

CoS traffic shaping is based on the subscriber downstream traffic rate that the ANCP agent receives from the access node and then passes to CoS. CoS can shape subscriber traffic at the level of the household or the session:

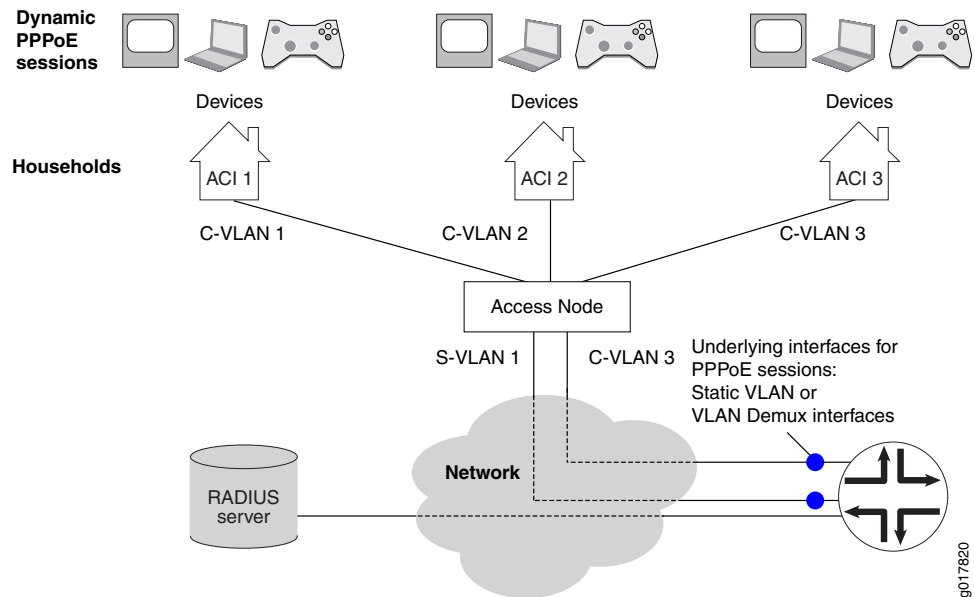
- Household shaping—Only aggregate traffic to the household is shaped. Household shaping results from applying a CoS traffic-control profile to the static VLAN or VLAN demux interface or to the interface set.
- Session shaping—The traffic rate to individual devices in the household is shaped. Session shaping results from specifying a CoS traffic-control profile in the dynamic PPPoE profile that creates the subscriber session. Depending on the network configuration, session shaping may employ shared priority queues to shape all sessions identically or individual priority queues to shape the sessions separately.

The following sections illustrate several possible configurations and lists the sequence of events for the ANCP operations in each case. Not every possible configuration is presented.

ANCP Network Using N:1 and 1:1 Configuration Models without Interface Sets

In this sample topology, two households are configured for one underlying static VLAN or VLAN demux interface (N:1; dual-tagged VLAN) and a single household is configured for another underlying interface (1:1; single-tagged VLAN) (Figure 1 on page 18). In addition to the unique ACI assigned by the access node, each household is further identified by the VLAN, which is mapped to the identifier in the ANCP agent configuration. CoS traffic shaping for sessions can employ only shared priority queues to shape all sessions identically; individual priority queues to shape the sessions separately are not supported.

Figure 1: Sample ANCP Topology Without Interface Sets (1:1 and N:1 Model)



Sequence of ANCP Events: Static VLAN or VLAN Demux Interfaces over Ethernet Without Interface Sets

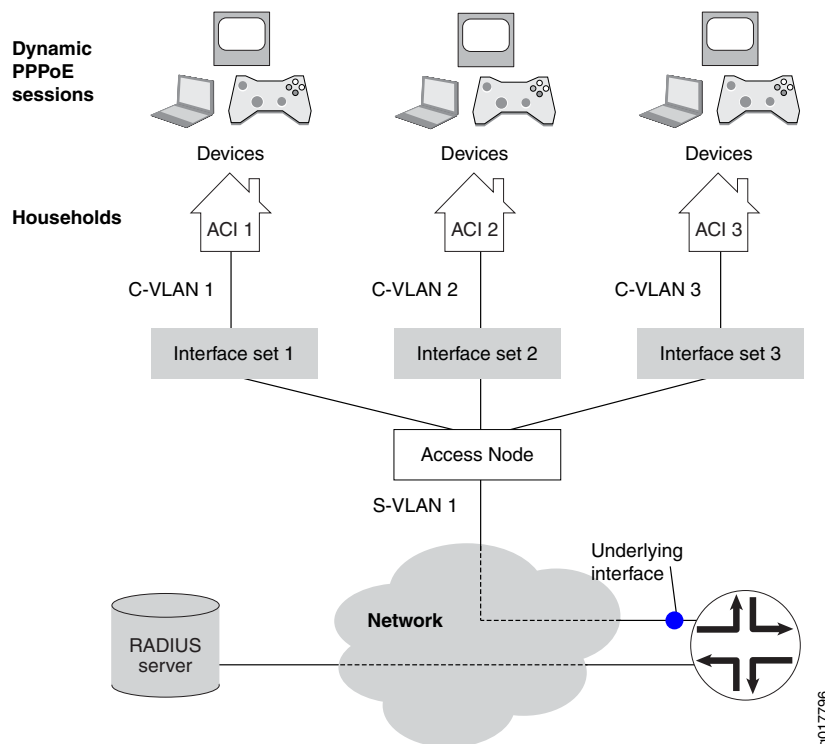
The following sequence of events is for the topology in [Figure 1 on page 18](#) with static VLAN interfaces over Ethernet without interface sets.

1. A network device in the household initiates PPPoE discovery.
2. PPPoE creates a dynamic PPPoE session on the underlying static VLAN or VLAN demux interface and applies the advisory options configured on the VLAN to the session.
3. The access node independently provides the ANCP agent with the ANCP DSL attributes for an access line identified by an ACI.
4. The ANCP agent sends CoS the adjusted downstream data rate for the static VLAN or demux VLAN mapped to the ACI. The ANCP agent stores all DSL attributes, including the adjusted upstream data rate, in the router's shared database.
5. AAA correlates the dynamic PPPoE session with the access line by matching the underlying interface of the session to the static VLAN or VLAN demux interface associated with the ACI in the ANCP agent configuration.
6. AAA retrieves the ANCP DSL attributes for the access line from the router's shared database and maps them to the Juniper Networks DSL VSAs in the RADIUS Access-Request and Accounting-Request messages. If the DSL attributes are unavailable, the session's advisory upstream and downstream data rates are mapped to the Upstream-Calculated-Qos-Rate VSA (26-142) and Downstream-Calculated-Qos-Rate (26-141) VSAs, respectively. These VSAs are then included in the RADIUS messages.

ANCP Network Using N:1 Configuration Model with Interface Sets

In this topology, multiple households are configured for each underlying static VLAN or VLAN demux interface (Figure 2 on page 20). The VLANs are dual-tagged. Each household includes several CPE devices that access the Internet. In addition to the unique ACI assigned by the access node, the household is further identified by the interface set. The interface set groups the dynamic PPPoE sessions for the individual subscriber devices. It is either explicitly configured in the dynamic PPPoE profile or specified in the RADIUS Access-Accept message during PPPoE session authentication. Session shaping can employ shared priority queues to shape all sessions identically or individual queues to shape the sessions separately.

Figure 2: Sample ANCP Topology with Interface Sets (N:1 Model)



In this N:1 model with interface sets, the access node must add the DSL Forum VSA to the PPPoE PADI and PADR discovery packets that it passes to the router during the establishment of dynamic PPPoE sessions. The VSA includes the ACI for the household. This inclusion enables AAA to correlate the PPPoE sessions with their respective subscriber access lines and DSL attributes during RADIUS authentication and accounting. If the ACI is not present, AAA cannot make the correlation and subsequently reports only the advisory upstream and downstream data rates to RADIUS Authentication and Accounting.

When the dynamic PPPoE profile is configured with the **\$junos-interface-set-name** predefined variable, the configuration of the access node, router, and RADIUS server must be synchronized with regard to the ACI and interface set:

- The RADIUS Access-Accept message must contain the Juniper Networks Qos-Interface-Set-Name VSA (26-130).
- The CoS Layer 2 configuration must explicitly identify the interface set that is named in the Qos-Interface-Set-Name VSA (26-130).
- The ANCP agent configuration must map an ACI to the interface set that is named in the Qos-Interface-Set-Name VSA (26-130).

Sequence of ANCP Events: Static VLAN Interfaces over Ethernet with Interface Sets

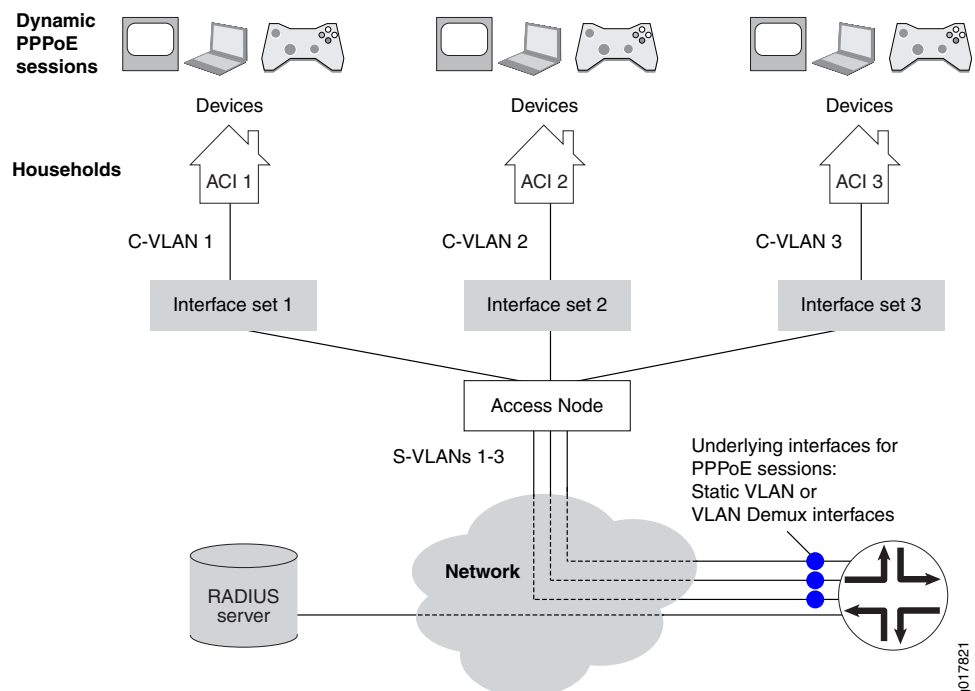
The following sequence of events is for the topology in [Figure 2 on page 20](#) with static VLAN interfaces over Ethernet with interface sets.

1. A network device in the household initiates PPPoE discovery.
2. The access node adds the DSL Forum VSA tag with the ACI for the household to the PPPoE PADI and PADR discovery packets. (The identifier is known to PPPoE as the agent circuit identifier.)
3. PPPoE creates a dynamic PPPoE session with the provided ACI on the underlying static VLAN and applies the advisory options configured on the VLAN to the session.
4. The access node independently provides the ANCP agent with the ANCP DSL attributes for an access line identified by an ACI.
5. The ANCP agent provides CoS with the adjusted downstream data rate for the interface set mapped to the ACI. The ANCP agent stores all ANCP DSL attributes, including the adjusted upstream and downstream data rates, in the router's shared database.
6. AAA correlates the dynamic PPPoE session with the access line by matching the session identifier received in the DSL Forum VSA to the ACI configured for the interface set in the ANCP agent configuration.
7. AAA retrieves the ANCP DSL attributes for the access line from the router's shared database and maps them to the Juniper Networks DSL VSAs in the RADIUS Access-Request and Accounting-Request messages. If the DSL attributes are unavailable, the session's advisory upstream and downstream data rates are mapped to the Upstream-Calculated-Qos-Rate VSA (26-142) and Downstream-Calculated-Qos-Rate (26-141) VSAs, respectively. These VSAs are then included in the RADIUS messages.
8. When authentication is completed, the dynamic PPPoE session is placed into the interface set configured in the dynamic PPPoE profile. The profile specifies a named interface set or the **\$junos-interface-set-name** predefined variable, which indicates that the interface set is named in the RADIUS Access-Accept message.

ANCP Network Using 1:1 Configuration Model with Interface Sets

In this topology, a single household is configured for each underlying static VLAN or VLAN demux interface (Figure 3 on page 22). The VLANs are dual-tagged. Each household includes several CPE devices that access the Internet. In addition to the unique ACI assigned by the access node, the household is further identified by the interface set. The interface set is either explicitly configured in the dynamic PPPoE profile or specified in the RADIUS Access-Accept message during PPPoE session authentication. Session shaping can employ shared priority queues to shape all sessions identically or individual queues to shape the sessions separately.

Figure 3: Sample ANCP Topology with Interface Sets (1:1 Model)



In this 1:1 model with interface sets, the ANCP agent configuration must map the underlying interface for the PPPoE sessions in an interface set to both the ACI and the interface set. This configuration enables AAA to correlate the PPPoE sessions with their respective subscriber access lines and DSL attributes during RADIUS authentication and accounting.

When the dynamic PPPoE profile is configured with the `$junos-interface-set-name` predefined variable, the configuration of the access node, router, and RADIUS server must be synchronized with regard to the ACI and interface set:

- The RADIUS Access-Accept message must contain the Juniper Networks Qos-Interface-Set-Name VSA (26-130).
- The CoS Layer 2 configuration must explicitly identify the interface set that is named in the Qos-Interface-Set-Name VSA (26-130).
- The ANCP agent configuration must map an ACI to the interface set that is named in the Qos-Interface-Set-Name VSA (26-130).

Sequence of ANCP Events: Static VLAN Demux Interfaces over Aggregated Ethernet with Interface Sets

The following sequence of events is for the topology in [Figure 3 on page 22](#) with static VLAN demux interfaces over aggregated Ethernet with interface sets.

1. A network device in the household initiates PPPoE discovery.
2. PPPoE creates a dynamic PPPoE session with the provided ACI on the underlying static VLAN demux interface and applies the advisory options configured on the VLAN to the session.
3. The access node independently provides the ANCP agent with the ANCP DSL attributes for an access line identified by an ACI.
4. The ANCP agent provides CoS with the adjusted downstream data rate for the interface set mapped to the ACI. The ANCP agent stores all ANCP DSL attributes, including the adjusted upstream and downstream data rates, in the router's shared database.
5. AAA correlates the dynamic PPPoE session with the access line by matching the underlying interface of the session to the underlying interface configured for the interface set in the ANCP agent configuration.
6. AAA retrieves the ANCP DSL attributes for the access line from the router's shared database and maps them to the Juniper Networks DSL VSAs in the RADIUS Access-Request and Accounting-Request messages. If the DSL attributes are unavailable, the session's advisory upstream and downstream data rates are mapped to the Upstream-Calculated-Qos-Rate VSA (26-142) and Downstream-Calculated-Qos-Rate (26-141) VSAs, respectively. These VSAs are then included in the RADIUS messages.
7. When authentication is completed, the dynamic PPPoE session is placed into the interface set configured in the dynamic PPPoE profile. The profile specifies a named interface set or the `$junos-interface-set-name` predefined variable, which indicates that the interface set is named in the RADIUS Access-Accept message.

Related Documentation

- [ANCP and the ANCP Agent Overview on page 3](#)
- [Configuring the ANCP Agent on page 29](#)
- [Example: Configuring an ANCP Network with Interface Sets and N:1 Static Demux VLANs over Aggregated Ethernet on page 43](#)

ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes

Digital Subscriber Line (DSL) attributes are RADIUS vendor-specific attributes (VSAs) that are defined by the DSL Forum in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*. The attributes transport DSL information that is not supported by standard RADIUS attributes and which conveys details about the associated DSL subscriber line and traffic. These attributes are contained as subattributes in the single DSL Forum VSA (IANA vendor ID 3561). An ANCP access node can provide this information to the router in a PPPoE PADI message during PPPoE subscriber discovery.

The access node can also report the same information about the DSL subscriber line and traffic information by means of the ANCP DSL TLVs or attributes carried in ANCP messages to the router. The ANCP attributes are defined in RFC 6320, *Protocol for Access Node Control Mechanism in Broadband Networks*. These ANCP DSL attributes correspond to Juniper Networks (IANA vendor ID 4874) DSL VSAs and to DSL Forum VSAs.

The router simply passes the DSL line and traffic information that it receives from the access node to the RADIUS server, without performing any parsing or manipulation. A RADIUS authentication or accounting message can contain any combination of the DSL Forum VSAs and the Juniper Networks DSL VSAs. You can configure the RADIUS access profile to exclude one or more individual attributes, or all DSL Forum attributes, from being included in RADIUS messages.

The DSL Forum attribute and subattributes received by the router during PPPOE and DHCP client discovery are not updated after discovery, whereas the equivalent ANCP DSL attributes are updated whenever there is a change to the access line.

[Table 6 on page 24](#) shows the relationship between the ANCP DSL attributes, Juniper Networks DSL VSAs, and DSL Forum VSAs.

Table 6: Mapping ANCP DSL Attributes to Juniper Networks DSL VSAs and DSL Forum VSAs

ANCP DSL Attribute Name	Juniper Networks VSA Name [Number]	DSL Forum VSA Name [Number]
Access-Aggregation-Circuit-ID-ASCII	Acc-Aggr-Cir-Id-Asc [26-112]	Access-Loop-Encapsulation [26-144]
Access-Aggregation-Circuit-ID-Binary	Acc-Aggr-Cir-Id-Bin [26-111]	Agent-Remote-Id [26-2]
Access-Loop-Circuit-ID	Acc-Loop-Cir-Id [26-110]	Agent-Circuit-Id [26-1]
Actual-Interleaving-Delay-Downstream	Act-Interlv-Delay-Dn [26-126]	Actual-Interleaving-Delay-Downstream [26-142]
Actual-Interleaving-Delay-Upstream	Act-Interlv-Delay-Up [26-124]	Actual-Interleaving-Delay-Upstream [26-140]
Actual-Net-Data-Rate-Downstream	<ul style="list-style-type: none"> L2C-Down-Stream-Data [26-93]—Unadjusted rate Act-Data-Rate-Dn [26-115]—Unadjusted rate Downstream-Calculated-Qos-Rate [26-141]—Rate as adjusted by ANCP 	Actual-Data-Rate-Downstream [26-130]
Actual-Net-Data-Rate-Upstream	<ul style="list-style-type: none"> L2C-Up-Stream-Data [26-92]—Unadjusted rate Act-Data-Rate-Up [26-114]—Unadjusted rate Upstream-Calculated-Qos-Rate [26-142]—Rate as adjusted by ANCP 	Actual-Data-Rate-Upstream [26-129]

Table 6: Mapping ANCP DSL Attributes to Juniper Networks DSL VSAs and DSL Forum VSAs (*continued*)

ANCP DSL Attribute Name	Juniper Networks VSA Name [Number]	DSL Forum VSA Name [Number]
Attainable-Net-Data-Rate-Downstream	Att-Data-Rate-Dn [26–118]	Attainable-Data-Rate-Downstream [26–134]
Attainable-Net-Data-Rate-Upstream	Att-Data-Rate-Up [26–117]	Attainable-Data-Rate-Upstream [26–133]
DSL-Line-State	DSL-Line-State [26–127]	–
DSL-Type	DSL-Type [26–128]	–
Maximum-Net-Data-Rate-Downstream	Max-Data-Rate-Dn [26–120]	Maximum-Data-Rate-Downstream [26–136]
Maximum-Net-Data-Rate-Upstream	Max-Data-Rate-Up [26–119]	Maximum-Data-Rate-Upstream [26–135]
Maximum-Interleaving-Delay-Downstream	Max-Interlv-Delay-Dn [26–125]	Maximum-Interleaving-Delay-Downstream [26–141]
Maximum-Interleaving-Delay-Upstream	Max-Interlv-Delay-Up [26–123]	Maximum-Interleaving-Delay-Upstream [26–139]
Minimum-Net-Low-Power-Data-Rate-Downstream	Min-LP-Data-Rate-Dn [26–122]	Minimum-Data-Rate-Downstream-Low-Power [26–138]
Minimum-Net-Low-Power-Data-Rate-Upstream	Min-LP-Data-Rate-Up [26–121]	Minimum-Data-Rate-Upstream-Low-Power [26–137]
Minimum-Net-Data-Rate-Downstream	Min-Data-Rate-Dn [26–116]	Minimum-Data-Rate-Downstream [26–132]
Minimum-Net-Data-Rate-Upstream	Min-Data-Rate-Up [26–115]	Minimum-Data-Rate-Upstream [26–131]

- Related Documentation**
- [Juniper Networks VSAs Supported by the AAA Service Framework](#)
 - [Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 40](#)

Preservation of CoS Shaping Across ANCP Agent Restarts

When the ANCP agent stops due to a process or GRES, CoS enforces the ANCP downstream shaping-rates until the CoS keepalive timer expires. When the timer expires, CoS reverts to the CoS shaping-rate configured for the interfaces.

You configure the CoS keepalive timer by including the **maximum-helper-restart-time seconds** statement at the **[edit protocols ancp]** hierarchy level. It specifies how much

time other daemons such as CoS wait for the ANCP agent to restart and is used to configure the CoS rate update keepalive timer.

The ANCP agent does not maintain TCP sessions from neighbors across the restart or GRES. When it restarts, it must re-establish sessions with neighbors and subscriber sessions before the timer expires. For all the re-established sessions, the ANCP agent updates CoS with the updated downstream shaping rates and provides DSL line attributes to the session database for AAA.

If CoS stops or restarts while ANCP is up, the ANCP agent retransmits all known subscriber downstream rates to CoS. Any existing adjusted shaping rates that have not been updated revert to the configured CoS shaping rates when the CoS restart timer expires.

**Related
Documentation**

- [ANCP and the ANCP Agent Overview on page 3](#)
- [Configuring the ANCP Agent on page 29](#)
- [Specifying How Long Processes Wait for the ANCP Agent Restart to Complete on page 35](#)

PART 2

Configuration

- [Configuration Overview on page 29](#)
- [Configuration Tasks for ANCP on page 31](#)
- [Example on page 43](#)
- [Configuration Statements on page 65](#)

CHAPTER 2

Configuration Overview

- [Configuring the ANCP Agent on page 29](#)

Configuring the ANCP Agent

You can configure the ANCP agent to enable a service-oriented Layer 3 edge device to discover information about the topology of a connected access network. The ANCP agent can also provide details about subscriber traffic and enable the adjustment of QoS traffic shaping for subscribers.

To configure the ANCP agent:

1. Specify each ANCP neighboring access node to be monitored and optionally configure neighbor parameters.

See [“Configuring ANCP Neighbors” on page 31](#).

2. Specify the subscribers reached by a VLAN or a set of VLANs through a particular access node.

See [“Associating an Access Node with Subscribers for ANCP Agent Operations” on page 32](#).

3. (Optional) Configure the adjacency timer.

See [“Specifying the Interval Between ANCP Adjacency Messages” on page 33](#).

4. (Optional) Specify the maximum number of discovery table entries that are accepted.

See [“Specifying the Maximum Number of Discovery Table Entries” on page 34](#).

5. (Optional) Configure the ANCP agent to work with an early IETF draft.

See [“Configuring the ANCP Agent for Backward Compatibility” on page 34](#).

6. (Optional) Configure the graceful restart timer.

See [“Specifying How Long Processes Wait for the ANCP Agent Restart to Complete” on page 35](#).

7. (Optional) Configure the ANCP agent to learn partition IDs from neighbors.

See [“Configuring the ANCP Agent to Learn ANCP Partition IDs” on page 35](#).

8. (Optional) Configure an adjustment factor per DSL line type for the downstream and upstream data rates that the ANCP agent reports to AAA.

See [“Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates”](#) on page 36.

9. (Optional) Configure the ANCP agent to report unadjusted downstream traffic rates to CoS.

See [“Configuring the ANCP Agent to Report Traffic Rates to CoS”](#) on page 37.

10. (Optional) Specify a recommended shaping rate to be applied by RADIUS to downstream or upstream traffic per ANCP interface.

See [“Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces”](#) on page 38.

11. (Optional) Configure AAA to Include or Exclude Juniper Networks DSL VSAs in RADIUS authentication and accounting messages.

See [“Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages”](#) on page 40.

12. (Optional) Configure AAA to send an immediate interim accounting update to the RADIUS server when AAA receives a rate change notification from the ANCP agent on the router.

See [“Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications”](#) on page 41.

13. (Optional) Configure trace options for troubleshooting the configuration.

See [“Tracing ANCP Agent Operations for Subscriber Access”](#) on page 137.

**Related
Documentation**

- [ANCP and the ANCP Agent Overview](#) on page 3
- [Triggering ANCP OAM to Test the Local Loop](#) on page 41

CHAPTER 3

Configuration Tasks for ANCP

- [Configuring ANCP Neighbors on page 31](#)
- [Associating an Access Node with Subscribers for ANCP Agent Operations on page 32](#)
- [Specifying the Interval Between ANCP Adjacency Messages on page 33](#)
- [Specifying the Maximum Number of Discovery Table Entries on page 34](#)
- [Configuring the ANCP Agent for Backward Compatibility on page 34](#)
- [Specifying How Long Processes Wait for the ANCP Agent Restart to Complete on page 35](#)
- [Configuring the ANCP Agent to Learn ANCP Partition IDs on page 35](#)
- [Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 36](#)
- [Configuring the ANCP Agent to Report Traffic Rates to CoS on page 37](#)
- [Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 38](#)
- [Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 40](#)
- [Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications on page 41](#)
- [Triggering ANCP OAM to Test the Local Loop on page 41](#)

Configuring ANCP Neighbors

You must configure each neighboring access node that you want the ANCP agent to monitor and potentially shape traffic for. Some neighbor settings override globally configured values.

To configure an ANCP neighbor:

1. Specify the IP address of the neighbor.

```
[edit protocols ancp]  
user@host# set neighbor 10.2.3.4
```

2. (Optional) Configure the neighbor to operate in a backward-compatible mode when it does not support the current IETF standard and the backward-compatible mode is not configured globally.

```
[edit protocols ancp neighbor 10.2.3.4]
```

```
user@host# set pre-ietf-mode
```

3. (Optional) Override the globally configured backward-compatible mode when the neighbor supports the current IETF standard.

```
[edit protocols ancp neighbor 10.2.3.4]  
user@host# set ietf-mode
```

4. (Optional) Configure the interval in seconds between ANCP adjacency messages exchanged with this neighbor.

```
[edit protocols ancp neighbor 10.2.3.4]  
user@host# set adjacency-timer 20
```

5. (Optional) Specify the maximum number of discovery table entries that are accepted from this neighbor.

```
[edit protocols ancp neighbor 10.2.3.4]  
user@host# set maximum-discovery-table-entries 10000
```

Related Documentation

- [Configuring the ANCP Agent on page 29](#)
- [Configuring the ANCP Agent for Backward Compatibility on page 34](#)
- [Specifying the Interval Between ANCP Adjacency Messages on page 33](#)
- [Specifying the Maximum Number of Discovery Table Entries on page 34](#)

Associating an Access Node with Subscribers for ANCP Agent Operations

The ANCP agent on the router uses the access loop circuit identifier (ACI) to distinguish individual ANCP subscribers. Because the agent uses the ACI to associate (map) each subscriber to an interface or interface set, each ACI must be unique across all ANCP neighbors connected to the router.



NOTE: In earlier Junos OS releases, we recommend that the ACIs be unique across all neighbors, but state that this is not required. When the ACIs are not unique in the earlier releases, you can configure the subscribers to be uniquely identified by associating the IP address of the neighbor with the subscriber's interface or interface-set. Starting in Junos OS Release 13.3, this configuration is no longer supported and the ACIs must be unique across your ANCP network.

The ACIs can be statically or dynamically configured. When the subscriber's DHCP or PPPoE discovery packets contain the ACI, then the agent can dynamically map it to the interface or interface set. Otherwise, the ACI must be statically configured. A static configuration overrides dynamic mapping of ACIs—and therefore subscribers—to interfaces or sets.

To associate an ACI with a set of VLAN interfaces for subscribers:

- Specify the name of the interface set and the unique ACI for the access node.


```
[edit protocols ancp interfaces]
user@host# set interface-set vlan5 access-identifier "dslam port 2/3"
```

To associate an ACI with a single VLAN:

- Specify the logical interface and the unique ACI for the access node.

```
[edit protocols ancp interfaces]
user@host# set ge-1/0/4.12 access-identifier "dslam port-2-10"
```

To associate an ACI with a static VLAN demux interface:

- Specify the logical interface and the unique ACI for the access node.

```
[edit protocols ancp interfaces]
user@host# set demux0.100 access-identifier aci_100_1_0
```

Related Documentation

- [Configuring the ANCP Agent on page 29](#)
- [interfaces on page 80](#)

Specifying the Interval Between ANCP Adjacency Messages

When the ANCP agent and a neighbor negotiate to establish an adjacency, each proposes a value for the interval between the adjacency messages that they exchange after it is established. The larger of the values proposed by the agent and the neighbor is selected for the interval between subsequent adjacency messages exchanged by the agent and the neighbor. You can specify the interval value that the ANCP agent proposes for either all neighbors or a specific neighbor.

To configure the proposed interval between ANCP adjacency messages for all neighbors:

- Specify the time in seconds.

```
[edit protocols ancp]
user@host# set adjacency-timer 20
```

To configure the proposed interval between ANCP adjacency messages for a specific neighbor:

- Specify the time in seconds.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set adjacency-timer 20
```

Related Documentation

- [Configuring the ANCP Agent on page 29](#)
- [Configuring ANCP Neighbors on page 31](#)

Specifying the Maximum Number of Discovery Table Entries

You can specify the maximum number of discovery table entries accepted from all neighbors or from a particular neighbor.

To configure the maximum number of entries for all neighbors:

- Specify the number of entries.

```
[edit protocols ancp]
user@host# set maximum-discovery-table-entries 5000
```

To configure the maximum number of entries for a specific neighbor:

- Specify the number of entries.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set maximum-discovery-table-entries 5000
```

- Related Documentation**
- [Configuring the ANCP Agent on page 29](#)
 - [Configuring ANCP Neighbors on page 31](#)

Configuring the ANCP Agent for Backward Compatibility

You can configure the ANCP agent to operate in a mode compatible with the protocol as it was initially proposed to operate. This backward-compatible or pre-IETF mode is compatible with Internet draft draft-wadhwa-gsmp-l2control-configuration-00.txt, *GSMP extensions for layer2 control (L2C)*. Setting this backward-compatible mode enables interoperation with devices that are not compatible with the later ANCP Internet drafts or RFC 6320, *Protocol for Access Node Control Mechanism in Broadband Networks*.

When this mode is configured globally for all neighbors, you can override it for a particular neighbor that supports the IETF draft or standard.

To configure the ANCP agent to operate in a backward-compatible mode for all neighbors:

- Specify the pre-IETF mode.

```
[edit protocols ancp]
user@host# set pre-ietf-mode
```

To configure the ANCP agent to operate in a backward-compatible mode for a specific neighbor:

- Specify the pre-IETF mode.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set pre-ietf-mode
```

- To override the globally configured backward-compatible mode for a specific neighbor:
Specify the IETF mode.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set ietf-mode
```

- Related Documentation**
- [Configuring the ANCP Agent on page 29](#)
 - [Configuring ANCP Neighbors on page 31](#)

Specifying How Long Processes Wait for the ANCP Agent Restart to Complete

You can specify how long other processes wait for the ANCP agent to restart. The ANCP agent sends a keepalive message to CoS at intervals equal to one-third the value of the maximum helper restart time. For example, when you configure the maximum restart time to 120 seconds, the ANCP agent sends a keepalive message every 40 seconds.

If CoS does not receive a keepalive message within the maximum helper restart time, it considers the ANCP agent to be down and immediately reverts any traffic shaping updates that were implemented as a result of ANCP agent monitoring to the configured values. Consequently, traffic to the subscribers is not effectively shaped, potentially resulting in traffic drops in the DSLAMs. The configured values are maintained until the ANCP agent comes back up and sends fresh traffic shaping updates to CoS.

To configure how long other processes wait for the ANCP agent to restart:

- Specify the time in seconds.

```
[edit protocols ancp]
user@host# set maximum-helper-restart-time 150
```

- Related Documentation**
- [Configuring the ANCP Agent on page 29](#)
 - [Configuring ANCP to Adjust CoS Traffic Shaping](#)

Configuring the ANCP Agent to Learn ANCP Partition IDs

By default, the ANCP agent expects ANCP partition IDs to be zero, meaning that the access node is not divided into logical partitions that can each form adjacencies with routers. You can configure the ANCP agent to support nonzero partition IDs. When you do so, the agent waits a configurable period to receive a SYN message from a neighbor during adjacency initiation. When the agent receives such a message, it uses the partition information contained in the Partition ID, PType, and PFlag fields to generate in turn a SYN message that it sends to the neighbor to continue adjacency negotiation.

To configure the ANCP agent to learn partition ID information from neighbors:

1. Enable partition ID learning.

```
[edit protocols ancp]
user@host# set gsmp-syn-wait
```

2. (Optional) Specify the maximum time the ANCP agent waits to receive a SYN message from a neighbor during the formation of an adjacency.

```
[edit protocols ancp]
user@host# set gsmp-syn-timeout seconds
```

For example, to enable partition ID learning and force the ANCP agent to wait 45 seconds for a SYN message:

```
[edit protocols ancp]
user@host# set gsmp-syn-wait
user@host# set gsmp-syn-timeout 45
```

**Related
Documentation**

- [Configuring the ANCP Agent on page 29](#)
- [ANCP and the ANCP Agent Overview on page 3](#)

Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates

The ANCP agent always reports both upstream and downstream rates to AAA. When a DSLAM calculates the data rate on the subscriber local loop, it ignores the additional headers on the DSL line that are associated with the overhead of the access mode (ATM or Ethernet). When the ANCP agent reports the net upstream data rate or the net downstream data rate, it includes the headers in its calculation and therefore reports a slightly higher value than that calculated by the DSLAM; this is the unadjusted data rate.

The ANCP agent also reports adjusted data rates to AAA. You can configure the agent to adjust the traffic rate to account for the header overhead by including one or more of the **qos-adjust-dsl-line-type** statements. Each of these statements sets an adjustment factor for a particular DSL line type that applies a percentage value to the total downstream and upstream data rates reported by the ANCP agent. That is, you configure the statements for all relevant line types, and the agent applies the appropriate adjustment when it identifies the line type for the interface. The adjustment factor applies globally for all subscribers of that DSL line type. By default, the ANCP agent applies an adjustment factor of 100 percent to all DSL lines, meaning that no adjustment is made. The ANCP agent simply passes on the DSL line rates that include the header information.



NOTE: The ANCP agent reports only unadjusted downstream data rates to CoS, and reports to CoS only when you include the **qos-adjust** statement at the **[edit protocols ancp]** hierarchy level.

To apply a global adjustment factor for DSL subscriber lines:

- Specify the adjustment factor percentage for the desired subscriber line.

```
[edit protocols ancp]
user@host# set qos-adjust-adsl adjustment-factor
user@host# set qos-adjust-adsl2 adjustment-factor
user@host# set qos-adjust-adsl2-plus adjustment-factor
user@host# set qos-adjust-sdsl adjustment-factor
user@host# set qos-adjust-vdsl adjustment-factor
user@host# set qos-adjust-vdsl2 adjustment-factor
```

- Related Documentation**
- [Configuring the ANCP Agent on page 29](#)
 - [ANCP and the ANCP Agent Overview on page 3](#)

Configuring the ANCP Agent to Report Traffic Rates to CoS

By default, the ANCP agent does not report the traffic rate on subscriber access lines to CoS. You can include the **qos-adjust** statement at the **[edit protocols ancp]** hierarchy level to configure the ANCP agent to report unadjusted or net downstream data rates to CoS for all subscribers in the network. This information enables CoS to subsequently shape the traffic on these access lines—but only if a shaping rate is configured in a CoS traffic-control profile for the access lines.

When a DSLAM calculates the data rate on the subscriber local loop, it ignores the additional headers on the DSL line that are associated with the overhead of the access mode (ATM or Ethernet). The unadjusted downstream data rate includes these headers in its calculation and therefore reports a slightly higher value than that calculated by the DSLAM. The ANCP agent also reports to CoS the traffic mode and the traffic rate overhead.



NOTE: The ANCP agent never reports upstream traffic rates to CoS, nor does it report adjusted downstream traffic rates to CoS.

If CoS does not receive a keepalive message within the maximum helper restart time, it considers the ANCP agent to be down and immediately reverts to the configured values any traffic shaping updates that were modified as a result of traffic reports from the ANCP agent. The configured values are maintained until the ANCP agent comes back up and sends fresh traffic updates to CoS.

However, if the ANCP agent remains running but loses the connection to a neighbor, CoS does not revert to its configured values. In this case, CoS changes the shaping rate for the subscriber traffic only if the ANCP agent restores the connection to that neighbor and reports new traffic rates to CoS or if you remove the **qos-adjust** statement.



NOTE: Always configure this statement for normal ANCP operations. You may want to disable it for debugging purposes.

To configure the ANCP agent to report unadjusted downstream traffic rates to CoS for traffic shaping:

- Specify that the ANCP agent reports traffic rates to CoS.

```
[edit protocols ancp]
user@host# set qos-adjust
```

- Related Documentation**
- [Traffic Rate Reporting and Adjustment by the ANCP Agent on page 10](#)
 - [Configuring the ANCP Agent on page 29](#)

- [ANCP and the ANCP Agent Overview on page 3](#)
- *Shaping Rate Adjustments for Subscriber Local Loops Overview*
- *Guidelines for Configuring Shaping-Rate Adjustments for Subscriber Local Loops*
- *Enabling Shaping-Rate Adjustments for Subscriber Local Loops*
- *Disabling Shaping-Rate Adjustments for Subscriber Local Loops*
- [Specifying How Long Processes Wait for the ANCP Agent Restart to Complete on page 35](#)
- [maximum-helper-restart-time on page 82](#)

Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces

When the access node sends information about the downstream and upstream calculated traffic rates for an interface, those values are used to shape the traffic sent to the interface so that it matches the subscriber local loop speed. You can specify recommended values that are used when the router does not receive this information from the access node. In this event, these recommended values are used as the default values for the following Juniper VSAs:

- Downstream-Calculated-Qos-Rate (IANA 4871, 26–141)—Conveys the transmit speed, which is the recommended traffic value in bits per second used for downstream traffic for an ANCP interface.
- Upstream-Calculated-Qos-Rate (IANA 4874, 26–142)—Conveys the receive speed, which is the recommended traffic value in bits per second used for upstream traffic for an ANCP interface.

You can configure the recommended rates either on static VLAN and VLAN demux interfaces, or you can specify them in a dynamic profile for dynamic VLAN and VLAN demux interfaces or interface sets.

To configure recommended traffic shaping values for a static interface:

1. Set the rate in bits per second for downstream traffic for the interface.

```
[edit interfaces interface-name unit logical-unit-number advisory-options]  
user@host# set downstream-rate rate
```
2. Set the rate in bits per second for upstream traffic for the interface.

```
[edit interfaces interface-name unit logical-unit-number advisory-options]  
user@host# set upstream-rate rate
```

For example, to set the recommended downstream rate to 16 Mbps and the recommended upstream rate to 1 Mbps on VLAN demux interface demux0.10301:

```
[edit interfaces demux0 unit 10301 advisory-options]  
user@host# set downstream-rate 16M  
user@host# set upstream-rate 1M
```

To configure recommended traffic shaping values for a dynamic interface:

1. Set the rate in bits per second for downstream traffic in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces $junos-interface-ifd-name unit
$junos-interface-unit advisory-options]
user@host# set downstream-rate rate
```

2. Set the rate in bits per second for upstream traffic in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces $junos-interface-ifd-name unit
$junos-interface-unit advisory-options]
user@host# set upstream-rate rate
```

For example, to configure the dynamic profile `ancp-dyn-vlan2` to set the recommended downstream rate to 10 Mbps and the recommended upstream rate to 1 Mbps on all interfaces in the dynamically created interface set:

```
[edit dynamic-profiles ancp-dyn-vlan2 interfaces $junos-interface-ifd-name unit
$junos-interface-unit advisory-options]
user@host# set downstream-rate 10M
user@host# set upstream-rate 1M
```

To configure recommended traffic shaping values for a dynamic interface set:

1. Set the rate in bits per second for downstream traffic in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces interface-set $junos-interface-set-name
interface $junos-interface-ifd-name advisory-options]
user@host# set downstream-rate rate
```

2. Set the rate in bits per second for upstream traffic in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces interface-set $junos-interface-set-name
interface $junos-interface-ifd-name advisory-options]
user@host# set upstream-rate rate
```

For example, to configure the dynamic profile `ancp-dyn-vlan1` to set the recommended downstream rate to 12 Mbps and the recommended upstream rate to 2 Mbps on all interfaces in the dynamically created interface set:

```
[edit dynamic-profiles ancp-dyn-vlan1 interfaces interface-set $junos-interface-set-name
interface $junos-interface-ifd-name advisory-options]
user@host# set downstream-rate 12M
user@host# set upstream-rate 2M
```

Related Documentation

- [Configuring the ANCP Agent on page 29](#)
- [Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 40](#)
- [Juniper Networks VSAs Supported by the AAA Service Framework](#)
- [ANCP and the ANCP Agent Overview on page 3](#)

Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages

You can include the **juniper-dsl-attributes** statement to configure AAA to add the set of Juniper Networks DSL VSAs to the RADIUS authentication and accounting request messages for subscribers. By default, these VSAs are not added to any RADIUS message. See [“ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes” on page 23](#) for a table of the Juniper Networks DSL VSAs.

After you have configured the inclusion of the Juniper Networks VSAs, you can subsequently exclude one or more of the VSAs from being transmitted. To do so, include the **exclude** statement at the **[edit access profile *profile-name* radius attributes]** hierarchy level, and specify which VSAs to exclude.

In contrast to the Juniper Networks DSL VSAs (vendor ID 4874), the DSL Forum VSA (vendor ID 3561) is added to all RADIUS messages by default. The DSL Forum VSA conveys individual DSL Forum attributes. See *DSL Forum Vendor-Specific Attributes* for a table of these VSAs. You can use the **exclude** statement at the **[edit access profile *profile-name* radius attributes]** hierarchy level to prevent this VSA from being included in any RADIUS message.

To add the Juniper Networks DSL VSAs to RADIUS messages:

- Configure the inclusion trigger.

```
[edit access profile profile-name radius options]
user@host# set juniper-dsl-attributes
```

To exclude specific Juniper Networks DSL VSAs from RADIUS messages:

- Configure the exclusion trigger.

```
[edit access profile profile-name radius attributes]
user@host# set exclude vsa-option
```

For example, to exclude the interleaving delay VSAs, configure the following statements:

```
[edit access profile profile-name radius attributes]
user@host# set exclude max-interlv-delay-dn
user@host# set excludemax-interlv-delay-up
```

To exclude the DSL Forum (RFC 4679) VSA from RADIUS messages:

- Configure the exclusion trigger.

```
[edit access profile profile-name radius attributes]
user@host# set exclude dsl-forum-attributes
```

Related Documentation

- [Configuring the ANCP Agent on page 29](#)
- [Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 38](#)
- [Juniper Networks VSAs Supported by the AAA Service Framework](#)
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 23](#)

- [ANCP and the ANCP Agent Overview on page 3](#)

Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications

When an ANCP neighbor reports a change in the upstream traffic rate or downstream traffic rate of an access line, the ANCP agent immediately passes the information to AAA. By default, AAA does not pass this information on to the RADIUS server until the next accounting update. However, you can configure AAA to report the rate change immediately.

When the access profile includes both the **ancp-speed-change-immediate-update** statement and the **update-interval** statement, receipt of the notification from the ANCP agent triggers AAA to send an interim update Accounting-Request message to the RADIUS server for the PPPoE and DHCP IP demux subscribers associated with that access line. The interim update request includes the new access line parameters and the adjusted upstream and downstream traffic rates.

To configure AAA to immediately send rate change information from the ANCP agent to the RADIUS server with interim accounting updates:

1. Enable interim accounting updates and configure the number of minutes between the updates.

```
[edit access profile profile-name accounting]
user@host# set update-interval minutes
```

2. Specify the immediate update.

```
[edit access profile profile-name accounting]
user@host# set ancp-speed-change-immediate-update
```

Related Documentation

- [Configuring the ANCP Agent on page 29](#)
- [Configuring Per-Subscriber Session Accounting](#)

Triggering ANCP OAM to Test the Local Loop

You can trigger ANCP OAM to perform a loopback test on the local loop between the access node and the CPE to help isolate simple faults. On an ATM-based local loop, the ANCP operation triggers the access node to generate ATM (F4/F5) loopback cells on the local loop. On an Ethernet-based local loop, the ANCP operation triggers the access node to generate an Ethernet loopback message on the local loop. When the test completes, the access node sends a message to the router with the results.

Issue the **request ancp oam neighbor** command from CLI operational mode to initiate testing of a local loop identified by the IP address or system name of the ANCP neighbor and the ACI for a subscriber on that access node.

Issue the **request ancp oam interface** command from CLI operational mode to initiate testing of a local loop identified by the ANCP interface or interface set associated with a subscriber and the ACI for a subscriber on that access node.

With both commands, you can also specify how many times the test must be run and how long the router waits for a response to the OAM request.

To initiate ANCP local loop testing:

- Identify the loop by the subscriber identifier and the neighbor's IP address; optionally specify how many times the test runs and the timeout period.

```
user@host> request ancp oam neighbor ip-address 192.168.32.5 subscriber "dslam  
port-2-10" count 5 timeout 600
```

- Identify the loop by the subscriber identifier and the neighbor's system name; optionally specify how many times the test runs and the timeout period.

```
user@host> request ancp oam neighbor system-name ba:ad:be:ef:10:10 subscriber  
"dslam port-2-10" count 10 timeout 600
```

- Identify the loop by the subscriber identifier and the interface associated with the subscriber; optionally specify how many times the test runs and the timeout period.

```
user@host> request ancp oam interface ge-1/0/2.12 identifier-string timeout 15
```

- Identify the loop by the subscriber identifier and the set of interfaces associated with the subscriber; optionally specify how many times the test runs and the timeout period.

```
user@host> request ancp oam interface interface-set vlan5 identifier-string count 3
```

**Related
Documentation**

- [ANCP and the ANCP Agent Overview on page 3](#)
- [Configuring the ANCP Agent on page 29](#)

CHAPTER 4

Example

- [Example: Configuring an ANCP Network with Interface Sets and N:1 Static Demux VLANs over Aggregated Ethernet on page 43](#)

Example: Configuring an ANCP Network with Interface Sets and N:1 Static Demux VLANs over Aggregated Ethernet

This example describes how to configure an ANCP network topology that manages subscriber access for several households by grouping individual devices into interface sets, providing access and services through one dedicated C-VLAN per household, and shaping traffic on a per-household basis. In this N:1 configuration, dual-tagged VLANs are configured over a single, underlying, static VLAN demux interfaces over aggregated Ethernet.

- [Requirements on page 43](#)
- [Overview on page 44](#)
- [Configuration on page 49](#)
- [Verification on page 61](#)

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Router with only MPCs installed for VLAN demux support
- RADIUS server
- DSLAM access node
- Junos OS Release 12.2 or later

Before you begin configuring the example, be sure you have:

- Thoroughly read and understood the following topics:
 - [ANCP and the ANCP Agent Overview on page 3](#)
 - [ANCP Operations in Different Network Configurations on page 15](#)
- Configured your access node.
- Configured your RADIUS server.

Overview

ANCP provides a means to configure, maintain, and monitor local access lines between access nodes (DSLAMs) and subscribers. Associated CoS configurations shape the downstream subscriber traffic. ANCP can enable more accurate traffic shaping by adjusting net data rates to discount the packet overhead of the access lines and then providing these adjusted rates to CoS.

The network topology in this example includes a dual-tagged (C-VLAN/S-VLAN) VLAN configuration over a static VLAN demux interface that is in turn configured over aggregated Ethernet for redundancy. This topology is an N:1 configuration model because—although each C-VLAN corresponds to one subscriber household—all the C-VLANs are configured over the same underlying VLAN demux interface. Multiple end-user devices in each household—or rather the dynamic PPPoE sessions established by each device—are grouped by household into interface sets. The grouping is accomplished by a separate dynamic profile configured for each C-VLAN. The ANCP agent configuration maps the ACI for the household's access line to an interface set. CoS applies a traffic-control profile to each interface set to shape the subscriber-directed traffic on a per-household basis. The CoS shaping rate is dynamically updated based upon the DSL attributes provided by the access node for each household's access line.

[Figure 4 on page 45](#) shows S-VLAN 103, configured on demux0, servicing the access node. C-VLANs 1, 2, and 3 each service a single household (subscriber). The respective households are identified by unique ACIs. The dynamic PPPoE sessions for devices in each household are grouped for monitoring and traffic shaping into interface sets 10301, 10302, and 10303.

Figure 4: N:1 ANCP Topology with Interface Sets and VLAN Demux Interface over Aggregated Ethernet

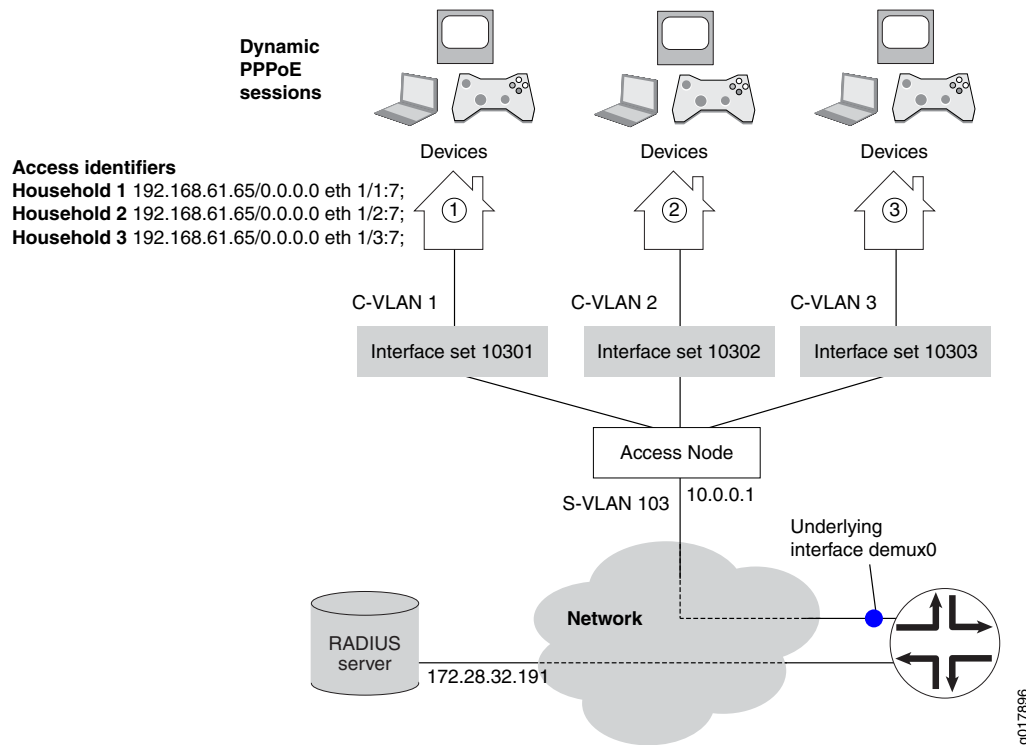


Table 7 on page 45 describes the configuration components used in this example.

Table 7: Configuration Components used in ANCP N:1 Topology Example with Interface Sets

Configuration Component or Property	Component Name or Setting	Description
Dynamic profiles	ancp-10301	Each profile defines the dynamic PPPoE session created when any of the devices for a particular subscriber household accesses the network.
	ancp-10302	
	ancp-10303	
		Each profile specifies the following:
		<ul style="list-style-type: none"> A set of interfaces in which the sessions are created. Dynamic instantiation of both the logical interfaces for the sessions and the underlying PPPoE logical interfaces on which the subscribers log in. CHAP and PAP authentication for the sessions. The interval between successive PPP keepalive messages. The loopback address for the dynamic PPPoE logical interfaces.

Table 7: Configuration Components used in ANCP N:1 Topology Example with Interface Sets (*continued*)

Configuration Component or Property	Component Name or Setting	Description
Predefined variables	\$junos-interface-unit	Instantiates the logical interface for each PPPoE session.
	\$junos-underlying-interface	Instantiates the logical underlying PPP interface on which each dynamic PPPoE logical interface is created when a subscriber logs in.

Table 7: Configuration Components used in ANCP N:1 Topology Example with Interface Sets (*continued*)

Configuration Component or Property	Component Name or Setting	Description
Interfaces	ae0	<p>Aggregated Ethernet interface that is the underlying interface for the VLAN demux interfaces.</p> <p>The interface includes the following configuration:</p> <ul style="list-style-type: none"> • CoS hierarchical scheduling. • Stacked VLAN tagging for all logical interfaces on top of ae0. • Link protection.
	demux0	VLAN demux interface that runs over the underlying aggregated Ethernet interface.
	demux0.10301	<p>VLAN demux logical interfaces that correspond to the C-VLANs for individual subscriber households.</p> <p>Each logical interface includes the following configuration:</p> <ul style="list-style-type: none"> • Inner (C-VLAN) and outer VLAN (S-VLAN) tags. • The underlying physical interface, ae0. • The dynamic profile that creates PPPoE sessions on the C-VLAN. • Downstream and upstream advisory traffic rates. • Proxy ARP and protection against duplicate sessions on the interface.
	demux0.10302	
	demux0.10303	
	ge-1/0/1	Primary member link in the aggregated Ethernet bundle.
	ge-1/0/2	Backup member link in the aggregated Ethernet bundle.
	lo0.0	Loopback interface for use in the access network. The loopback interface is automatically used for unnumbered interfaces.
	pp0	PPP interface on which the PPPoE subscriber logical interfaces are created.

Table 7: Configuration Components used in ANCP N:1 Topology Example with Interface Sets (*continued*)

Configuration Component or Property	Component Name or Setting	Description
Interface sets	10301	Set of interfaces in which the sessions for the devices in a particular household are created. Each interface set is specified in a dynamic profile for that household. ANCP associates each interface set with an ACI and a VLAN demux logical interface (C-VLAN). CoS applies a traffic-control profile to each interface set.
	10302	
	10303	
Advisory traffic rates	downstream-rate	Recommended rate for downstream traffic in the absence of traffic rate information from the access node.
	upstream-rate	Recommended rate for upstream traffic in the absence of traffic rate information from the access node.
Traffic-control profile	tcp1	CoS profile that shapes the downstream subscriber traffic rate; in this example, shaping is adjusted for ATM packet overhead. The profile is applied to the interface sets.
IP addresses	10.0.0.1	Address of the ANCP access node that monitors the subscriber households.
	10.50.0.1/28	Address of the loopback interface, lo0.
	172.28.32.191	Address of the RADIUS accounting server and authentication server.
Access circuit loop identifiers	192.168.61.65/0.0.0.0 eth 1/1:7;	Identifier for the local access circuit from the access node to the subscriber household. It identifies the household. ANCP associates each identifier with an interface set.
	192.168.61.65/0.0.0.0 eth 1/2:7;	
	192.168.61.65/0.0.0.0 eth 1/3:7;	

The ANCP agent configuration includes the following elements:

- The IP address for the access node (DSLAM) is specified as 10.0.0.1. The interval between ANCP adjacency messages sent between neighbors is set to 5 seconds.
- The ANCP agent is enabled to report adjusted data rates to CoS to improve the accuracy of downstream traffic shaping. The ANCP agent adjusts the net data rates for ADSL lines by ninety percent and for ADSL2 lines by ninety-five percent.
- Each interface set is associated with both the ACI unique to the subscriber household and the relevant underlying VLAN demux interface.

The RADIUS configuration on the router includes the following elements:

- The IP address (172.28.32.191) for the authentication and accounting server, as well as the secret password for accessing the server.
- The subscriber access profile, radius-profile, specifies that RADIUS is used for authentication.
- Juniper Networks DSL VSAs are included in RADIUS request messages, but the DSL Forum VSA attributes are excluded from RADIUS messages
- Accounting sessions are configured to be recognized in decimal format.

Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure an ANCP network with static N:1 demux VLANs to the subscriber households, perform these tasks:

- [Configuring the Dynamic PPPoE Profiles on page 51](#)
- [Configuring the Static VLAN Demux Interface over Aggregated Ethernet on page 53](#)
- [Configuring Class of Service on page 57](#)
- [Configuring ANCP on page 58](#)
- [Configuring RADIUS Authentication and Accounting on page 59](#)

CLI Quick Configuration

To quickly configure the ANCP network described in this example, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
# Dynamic Profiles
edit dynamic-profiles ancp-10301
set interfaces interface-set 10301 interface pp0 unit "$junos-interface-unit"
edit interfaces pp0 unit "$junos-interface-unit"
set ppp-options chap
set ppp-options pap
set pppoe-options underlying-interface "$junos-underlying-interface"
set keepalives interval 30
set family inet unnumbered-address lo0.0
top
edit dynamic-profiles ancp-10302
set interfaces interface-set 10302 interface pp0 unit "$junos-interface-unit"
edit interfaces pp0 unit "$junos-interface-unit"
set ppp-options chap
set ppp-options pap
set pppoe-options underlying-interface "$junos-underlying-interface"
set keepalives interval 30
set family inet unnumbered-address lo0.0
top
edit dynamic-profiles ancp-10303
set interfaces interface-set 10303 interface pp0 unit "$junos-interface-unit"
edit interfaces pp0 unit "$junos-interface-unit"
```

```
set ppp-options chap
set ppp-options pap
set pppoe-options underlying-interface "$junos-underlying-interface"
set keepalives interval 30
set family inet unnumbered-address lo0.0
top
#
# Aggregated Ethernet Interfaces and VLAN Demux Interfaces
set interfaces ge-1/0/1 hierarchical-scheduler
set interfaces ge-1/0/1 gigether-options 802.3ad ae0
set interfaces ge-1/0/1 gigether-options 802.3ad primary
set interfaces ge-1/0/2 hierarchical-scheduler
set interfaces ge-1/0/2 gigether-options 802.3ad ae0
set interfaces ge-1/0/2 gigether-options 802.3ad backup
set interfaces ae0 hierarchical-scheduler
set interfaces ae0 stacked-vlan-tagging
set interfaces ae0 aggregated-ether-options link-protection
set interfaces demux0 unit 10301 proxy-arp
set interfaces demux0 unit 10301 vlan-tags outer 103
set interfaces demux0 unit 10301 vlan-tags inner 1
set interfaces demux0 unit 10301 demux-options underlying-interface ae0
set interfaces demux0 unit 10301 family pppoe duplicate-protection
set interfaces demux0 unit 10301 family pppoe dynamic-profile ancp-10301
set interfaces demux0 unit 10301 advisory-options downstream-rate 16m
set interfaces demux0 unit 10301 advisory-options upstream-rate 1m
set interfaces demux0 unit 10302 proxy-arp
set interfaces demux0 unit 10302 vlan-tags outer 103
set interfaces demux0 unit 10302 vlan-tags inner 2
set interfaces demux0 unit 10302 demux-options underlying-interface ae0
set interfaces demux0 unit 10302 family pppoe duplicate-protection
set interfaces demux0 unit 10302 family pppoe dynamic-profile ancp-10302
set interfaces demux0 unit 10302 advisory-options downstream-rate 16m
set interfaces demux0 unit 10302 advisory-options upstream-rate 1m
set interfaces demux0 unit 10303 proxy-arp
set interfaces demux0 unit 10303 vlan-tags outer 103
set interfaces demux0 unit 10303 vlan-tags inner 3
set interfaces demux0 unit 10303 demux-options underlying-interface ae0
set interfaces demux0 unit 10303 family pppoe duplicate-protection
set interfaces demux0 unit 10303 family pppoe dynamic-profile ancp-10303
set interfaces demux0 unit 10303 advisory-options downstream-rate 16m
set interfaces demux0 unit 10303 advisory-options upstream-rate 1m
set interfaces lo0 unit 0 family inet address 10.50.0.1/28
top
#
# Class of Service
edit class-of-service
set traffic-control-profiles tcp1 shaping-rate 16m
set traffic-control-profiles tcp1 overhead-accounting cell-mode
set interfaces interface-set 10301 output-traffic-control-profile tcp1
set interfaces interface-set 10302 output-traffic-control-profile tcp1
set interfaces interface-set 10303 output-traffic-control-profile tcp1
top
#
# ANCP
edit protocols ancp
set traceoptions file ancpd
```

```

set traceoptions file size 512m
set traceoptions flag config
set traceoptions flag cos
set qos-adjust
set adjacency-timer 5
set maximum-helper-restart-time 90
set qos-adjust-adsl 90
set qos-adjust-adsl2 95
set interfaces interface-set 10301 access-identifier "192.168.61.65/0.0.0.0 eth 1/1:7;"
set interfaces interface-set 10302 access-identifier "192.168.61.65/0.0.0.0 eth 1/2:7;"
set interfaces interface-set 10303 access-identifier "192.168.61.65/0.0.0.0 eth 1/3:7;"
set interfaces interface-set 10301 underlying-interface demux0.10301
set interfaces interface-set 10302 underlying-interface demux0.10302
set interfaces interface-set 10303 underlying-interface demux0.10303
set neighbor 10.0.0.1
top
#
# RADIUS
edit access
set radius-server 172.28.32.191 secret "$9$MUeL7VgoGqmTwYmTz3tpWLx"
edit access profile radius-profile
set authentication-order radius
set radius authentication-server 172.28.32.191
set radius accounting-server 172.28.32.191
set radius options accounting-session-id-format decimal
set radius options juniper-dsl-attributes
set radius attributes exclude dsl-forum-attributes access-request
set radius attributes exclude dsl-forum-attributes accounting-start
set radius attributes exclude dsl-forum-attributes accounting-stop
top

```

Configuring the Dynamic PPPoE Profiles

Step-by-Step Procedure

In this procedure, you configure a dynamic profile for each C-VLAN: ancp-10301, ancp-10302, and ancp-10303.

1. Configure the interface set that the PPPoE sessions on this C-VLAN are placed in.

```

[edit dynamic-profiles ancp-10301]
user@host1# edit interfaces interface-set 10301

```
2. Configure the logical interfaces to be dynamically instantiated for the interface set.

```

[edit dynamic-profiles ancp-10301 interfaces interface-set 10301]
user@host1# set interface pp0 unit "$junos-interface-unit"

```
3. Configure CHAP and PAP authentication as properties of the dynamic PPPoE logical interfaces.

```

[edit dynamic-profiles ancp-10301 interfaces pp0 unit "$junos-interface-unit"]
user@host1# set ppp-options chap
user@host1# set ppp-options pap

```
4. Configure the logical underlying interface on which the router creates the dynamic PPPoE logical interface; this is the interface on which the subscriber logs in.

```

[edit dynamic-profiles ancp-10301 interfaces pp0 unit "$junos-interface-unit"]
user@host1# set pppoe-options underlying-interface "$junos-underlying-interface"

```

5. Specify the interval between successive keepalive requests.

```
[edit dynamic-profiles ancp-10301 interfaces pp0 unit "$junos-interface-unit"]
user@host1# set keepalives interval 30
```

6. Configure the IPv4 protocol family and that the local (unnumbered) address can be derived from the loopback address for the dynamic PPPoE logical interfaces.

```
[edit dynamic-profiles ancp-10301 interfaces pp0 unit "$junos-interface-unit"]
user@host1# set family inet unnumbered-address lo0.0
```

7. Repeat Steps 1 through 6 for the second dynamic profile, ancp-10302, and the third dynamic profile, ancp-10303.

Results From configuration mode, confirm the dynamic profile configuration by entering the **show dynamic-profiles** command.

```
[edit]
user@host# show dynamic-profiles
ancp-10301 {
  interfaces {
    interface-set 10301 {
      interface pp0 {
        unit "$junos-interface-unit";
      }
    }
  }
  pp0 {
    unit "$junos-interface-unit" {
      ppp-options {
        chap;
        pap;
      }
      pppoe-options {
        underlying-interface "$junos-underlying-interface";
      }
      keepalives interval 30;
      family inet {
        unnumbered-address lo0.0;
      }
    }
  }
}
ancp-10302 {
  interfaces {
    interface-set 10302 {
      interface pp0 {
        unit "$junos-interface-unit";
      }
    }
  }
  pp0 {
    unit "$junos-interface-unit" {
      ppp-options {
        chap;
        pap;
      }
    }
  }
}
```

When you are done configuring the device, enter **commit** from configuration mode.

Step-by-Step Procedure

1. Enable hierarchical scheduling on this interface.

```
[edit interfaces ge-1/0/1]  
user@host1# set hierarchical-scheduler
```
2. Specify this interface as the primary member of the aggregated Ethernet bundle.

```
[edit interfaces ge-1/0/1]  
user@host1# set ggeth-opts 802.3ad ae0 primary
```
3. Enable hierarchical scheduling on a second interface.

```
[edit interfaces ge-1/0/2]  
user@host1# set hierarchical-scheduler
```
4. Specify this interface as the backup member of the aggregated Ethernet bundle.

```
[edit interfaces ge-1/0/2]
```

```
user@host1# set gigether-options 802.3ad ae0 backup
```

5. Enable hierarchical scheduling on the aggregated Ethernet interface.

```
[edit interfaces ae0]  
user@host1# set hierarchical-scheduler
```

6. Enable stacked VLAN tagging for all logical interfaces on the aggregated Ethernet interface.

```
[edit interfaces ae0]  
user@host1# set stacked-vlan-tagging
```

7. Enable link protection as a property of the aggregated Ethernet interface.

```
[edit interfaces ae0]  
user@host1# set aggregated-ether-options link-protection
```

8. Configure VLAN demux interface demux0.10301.

- a. Configure the router to respond to ARP requests on the interface.

```
[edit interfaces demux0 unit 10301]  
user@host1# set proxy-arp
```

- b. Configure the outer VLAN tag to identify the access node (S-VLAN) and the inner VLAN tag to identify the subscriber port on the access node (C-VLAN).

```
[edit interfaces demux0 unit 10301]  
user@host1# set vlan tags outer 103 inner 1
```

- c. Specify that the VLAN demux interface runs on the underlying aggregated Ethernet interface.

```
[edit interfaces demux0 unit 10301]  
user@host1# set demux-options underlying-interface ae0
```

- d. Prevent multiple PPPoE sessions from being created for the same PPPoE subscriber on this VLAN demux interface.

```
[edit interfaces demux0 unit 10301]  
user@host1# set family pppoe duplicate-protection
```

- e. Configure the dynamic profile that is instantiated on the VLAN demux interface.

```
[edit interfaces demux0 unit 10301]  
user@host1# set family pppoe dynamic-profile ancp-10301
```

- f. Configure the recommended upstream and downstream traffic rates.

```
[edit interfaces demux0 unit 10301]  
user@host1# set advisory-options upstream-rate 1m  
user@host1# set advisory-options downstream-rate 16m
```

9. Configure VLAN demux interface demux0.10302.

- a. Configure the router to respond to ARP requests on the interface.

```
[edit interfaces demux0 unit 10302]  
user@host1# set proxy-arp
```

- b. Configure the outer VLAN tag to identify the access node (S-VLAN) and the inner VLAN tag to identify the subscriber port on the access node (C-VLAN).

```
[edit interfaces demux0 unit 10302]
user@host1# set vlan tags outer 103 inner 2
```

- c. Specify that the VLAN demux interface runs on the underlying aggregated Ethernet interface.

```
[edit interfaces demux0 unit 10302]
user@host1# set demux-options underlying-interface ae0
```

- d. Prevent multiple PPPoE sessions from being created for the same PPPoE subscriber on this VLAN demux interface.

```
[edit interfaces demux0 unit 10302]
user@host1# set family pppoe duplicate-protection
```

- e. Configure the dynamic profile that is instantiated on the VLAN demux interface.

```
[edit interfaces demux0 unit 10302]
user@host1# set family pppoe dynamic-profile ancp-10302
```

- f. Configure the recommended upstream and downstream traffic rates.

```
[edit interfaces demux0 unit 10302]
user@host1# set advisory-options upstream-rate 1m
user@host1# set advisory-options downstream-rate 16m
```

- 10. Configure VLAN demux interface demux0.10303.

- a. Configure the router to respond to ARP requests on the interface.

```
[edit interfaces demux0 unit 10303]
user@host1# set proxy-arp
```

- b. Configure the outer VLAN tag to identify the access node (S-VLAN) and the inner VLAN tag to identify the subscriber port on the access node (C-VLAN).

```
[edit interfaces demux0 unit 10303]
user@host1# set vlan tags outer 103 inner 3
```

- c. Specify that the VLAN demux interface runs on the underlying aggregated Ethernet interface.

```
[edit interfaces demux0 unit 10303]
user@host1# set demux-options underlying-interface ae0
```

- d. Prevent multiple PPPoE sessions from being created for the same PPPoE subscriber on this VLAN demux interface.

```
[edit interfaces demux0 unit 10303]
user@host1# set family pppoe duplicate-protection
```

- e. Configure the dynamic profile that is instantiated on the VLAN demux interface.

```
[edit interfaces demux0 unit 10303]
user@host1# set family pppoe dynamic-profile ancp-10303
```

- f. Configure the recommended upstream and downstream traffic rates.

```
[edit interfaces demux0 unit 10303]
user@host1# set advisory-options upstream-rate 1m
user@host1# set advisory-options downstream-rate 16m
```

- 11. Configure the IPv4 protocol family and the address of the loopback interface.

```
[edit interfaces lo0]
user@host1# set unit 0 family inet address 10.50.0.1/28
```

Results From configuration mode, confirm the static VLAN demux configuration by entering the **show interfaces** command.

```
[edit]
user@host# show interfaces
ge-1/0/1 {
  hierarchical-scheduler;
  gigether-options {
    802.3ad {
      ae0;
      primary;
    }
  }
}
ge-1/0/2 {
  hierarchical-scheduler;
  gigether-options {
    802.3ad {
      ae0;
      backup;
    }
  }
}
ae0 {
  hierarchical-scheduler;
  stacked-vlan-tagging;
  aggregated-ether-options {
    link-protection;
  }
}
demux0 {
  unit 10301 {
    proxy-arp;
    vlan-tags outer 103 inner 1;
    demux-options {
      underlying-interface ae0;
    }
    family pppoe {
      duplicate-protection;
      dynamic-profile ancp-10301;
    }
    advisory-options {
      downstream-rate 16m;
      upstream-rate 1m;
    }
  }
  unit 10302 {
    proxy-arp;
    vlan-tags outer 103 inner 2;
    demux-options {
      underlying-interface ae0;
    }
  }
}
```



```

family pppoe {
    duplicate-protection;
    dynamic-profile ancp-10302;
}
advisory-options {
    downstream-rate 16m;
    upstream-rate 1m;
}
}
unit 10303 {
    proxy-arp;
    vlan-tags outer 103 inner 3;
    demux-options {
        underlying-interface ae0;
    }
    family pppoe {
        duplicate-protection;
        dynamic-profile ancp-10303;
    }
    advisory-options {
        downstream-rate 16m;
        upstream-rate 1m;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.50.0.1/28
        }
    }
}
}

```

When you are done configuring the device, enter **commit** from configuration mode.

Configuring Class of Service

- | | |
|-------------------------------|---|
| Step-by-Step Procedure | <ol style="list-style-type: none"> Configure the traffic-control profile with the shaping rate and specify the overhead accounting mode to account for ATM cell encapsulation.

 <pre> [edit class-of-service] user@host1# set traffic-control-profiles tcp1 shaping-rate 16m user@host1# set traffic-control-profiles tcp1 overhead-accounting cell-mode </pre> Apply the traffic-control profile to the interface sets.

 <pre> [edit class-of-service] user@host1# set interfaces interface-set 10301 output-traffic-control-profile tcp1 user@host1# set interfaces interface-set 10302 output-traffic-control-profile tcp1 user@host1# set interfaces interface-set 10303 output-traffic-control-profile tcp1 </pre> |
| Results | <p>From configuration mode, confirm the class of service configuration by entering the show class-of-service command.</p> <pre> [edit] user@host# show class-of-service </pre> |

```
traffic-control-profiles {
  tcp1 {
    shaping-rate 16m;
    overhead-accounting cell-mode;
  }
}
interfaces {
  interface-set 10301 {
    output-traffic-control-profile tcp1;
  }
  interface-set 10302 {
    output-traffic-control-profile tcp1;
  }
  interface-set 10303 {
    output-traffic-control-profile tcp1;
  }
}
```

When you are done configuring the device, enter **commit** from configuration mode.

Configuring ANCP

Step-by-Step Procedure

1. Configure the access node address.

```
[edit protocols ancp]
user@host1# set neighbor 10.0.0.1
```
2. Configure the ANCP agent to report adjusted downstream traffic rates to CoS.

```
[edit protocols ancp]
user@host1# set qos-adjust
```
3. Specify an overhead adjustment of the traffic on ADSL and ADSL2 lines to 90 percent and 95 percent, respectively, of the net data rate.

```
[edit protocols ancp]
user@host1# set qos-adjust-adsl 90
user@host1# set qos-adjust-adsl2 95
```
4. Specify an interval of 5 seconds between adjacency messages sent to all ANCP neighbors.

```
[edit protocols ancp]
user@host1# set adjacency-timer 5
```
5. Associate the ACI with the interface sets for each C-VLAN.

```
[edit protocols ancp]
user@host1# set interfaces interface-set 10301 access-identifier
"192.168.61.65/0.0.0.0 eth 1/1:7;"
user@host1# set interfaces interface-set 10302 access-identifier
"192.168.61.65/0.0.0.0 eth 1/2:7;"
user@host1# set interfaces interface-set 10303 access-identifier
"192.168.61.65/0.0.0.0 eth 1/3:7;"
```
6. Specify the underlying interface for the interface sets.

```
[edit protocols ancp]
user@host1# set interfaces interface-set 10301 underlying-interface demux0.10301
```

```

user@host1# set interfaces interface-set 10302 underlying-interface demux0.10302
user@host1# set interfaces interface-set 10303 underlying-interface demux0.10303

```

7. Configure the size of the ANCP trace log files.

```

[edit protocols ancp traceoptions]
user@host1# set file ancpd size 512m

```

8. Configure flags for tracing ANCP configuration and CoS operations.

```

[edit protocols ancp traceoptions]
user@host1# set flag config
user@host1# set flag cos

```

Results From configuration mode, confirm the ANCP agent configuration by entering the **show ancp** command.

```

[edit]
user@host# show ancp
traceoptions {
  file ancpd size 512m;
  flag config;
  flag cos;
}
qos-adjust;
adjacency-timer 5;
qos-adjust-adsl 90;
qos-adjust-adsl2 95;
interfaces {
  interface-set {
    10301 {
      access-identifier "192.168.61.65/0.0.0.0 eth 1/1:7;";
      underlying-interface demux0.10301;
    }
    10302 {
      access-identifier "192.168.61.65/0.0.0.0 eth 1/2:7;";
      underlying-interface demux0.10302;
    }
    10303 {
      access-identifier "192.168.61.65/0.0.0.0 eth 1/3:7;";
      underlying-interface demux0.10303;
    }
  }
}
neighbor 10.0.0.1;

```

When you are done configuring the device, enter **commit** from configuration mode.

Configuring RADIUS Authentication and Accounting

Step-by-Step Procedure

1. Configure the password for the RADIUS server.

```

[edit access]
user@host1# set radius-server 172.28.32.191 secret
"$9$MUeL7VgoGqmTwYmTz3tpWLx"

```

2. Specify that RADIUS is used to authenticate subscribers.

```
[edit access]
user@host1# set profile radius-profile authentication-order radius
```

3. Configure the RADIUS authentication and accounting server.

```
[edit access]
user@host1# set profile radius-profile radius authentication-server 172.28.32.191
user@host1# set profile radius-profile radius accounting-server 172.28.32.191
```

4. Configure options for the RADIUS server: The format used to identify the accounting session and that Juniper Networks DSL VSAs are added to RADIUS request messages.

```
[edit access]
user@host1# set profile radius-profile radius options accounting-session-id-format
decimal
user@host1# set profile radius-profile radius options juniper-dsl-attributes
```

5. Exclude DSL Forum VSA attributes from being included in RADIUS messages.

```
[edit access]
user@host1# set profile radius-profile radius attribute exclude dsl-forum-attributes
access-request
user@host1# set profile radius-profile radius attribute exclude dsl-forum-attributes
accounting-start
user@host1# set profile radius-profile radius attribute exclude dsl-forum-attributes
accounting-stop
```

Results From configuration mode, confirm the RADIUS configuration by entering the **show access** command.

```
[edit]
user@host# show access
radius-server {
  172.28.32.191 secret "$9$MUeL7VgoGqmTwYmTz3tpWLx"; ## SECRET-DATA
}
profile radius-profile {
  radius {
    authentication-server 172.28.32.191;
    accounting-server 172.28.32.191;
    options {
      accounting-session-id-format decimal;
      juniper-dsl-attributes;
    }
    attributes {
      exclude {
        dsl-forum-attributes [ access-request accounting-start accounting-stop ];
      }
    }
  }
}
```

When you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying the Aggregated Ethernet Interface Configuration on page 61](#)
- [Verifying the Traffic Scheduling and Shaping Parameters for the Interface Set on page 61](#)
- [Verifying the demux0 Interface Configuration on page 62](#)
- [Verifying the pp0 Interface Configuration on page 62](#)
- [Verifying the ANCP Agent Configuration on page 63](#)

Verifying the Aggregated Ethernet Interface Configuration

Purpose Verify that the interface values match your configuration, the link is up, and traffic is flowing.

Action From operational mode, enter the **show interfaces redundancy** command.

```
user@host> show interfaces redundancy
Interface  State           Last change  Primary    Secondary  Current status
ae0        On primary                ge-1/0/1    ge-1/0/2    both up
```

From operational mode, enter the **show interfaces ae0** command.

```
user@host> show interfaces ae0
Physical interface: ae0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 606
  Link-level type: Ethernet, MTU: 1522, Speed: 1Gbps, BPDU Error: None,
  MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
  Flow control: Disabled, Minimum links needed: 1, Minimum bandwidth needed: 0
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Current address: 00:1f:12:b8:ef:c0, Hardware address: 00:1f:12:b8:ef:c0
  Last flapped   : 2012-03-11 13:24:18 PST (2d 03:34 ago)
  Input rate     : 1984 bps (2 pps)
  Output rate    : 0 bps (0 pps)
```

```
Logical interface ae0.32767 (Index 69) (SNMP ifIndex 709)
  Flags: SNMP-Traps 0x4004000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2
  Statistics          Packets      pps      Bytes      bps
  Bundle:
    Input :           371259         2    46036116    1984
    Output:              0         0         0         0
  Protocol multiservice, MTU: Unlimited
  Flags: Is-Primary
```

Meaning The **show interfaces redundancy** output shows the redundant link configuration and that both link interfaces are up. The **show interfaces ae0** output shows that the aggregated Ethernet interface is up and that traffic is being received on the logical interface.

Verifying the Traffic Scheduling and Shaping Parameters for the Interface Set

Purpose Verify that the traffic scheduling and shaping parameters are configured and applied properly.

Action user@host> show class-of-service

Verifying the demux0 Interface Configuration

Purpose Verify that the VLAN demux interface displays the configured PPPoE family attributes and the member links in the aggregated Ethernet bundle.

Action From operational mode, enter the **show interfaces demux0** command for each VLAN.

```
user@host> show interfaces demux0.10301
Logical interface demux0.10301 (Index 76) (SNMP ifIndex 61160)
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ]
  Encapsulation: ENET2
  Demux:
    Underlying interface: ae0 (Index 199)
  Link:
    ge-1/0/1
    ge-1/0/2
  Input packets : 2
  Output packets: 18575
  Protocol pppoe
    Dynamic Profile: ancp-10301,
    Service Name Table: None,
    Max Sessions: 16000, Duplicate Protection: On,
    AC Name: pppoe-server-1
```

Alternatively, you can enter **show pppoe underlying-interfaces detail** to display the state and PPPoE family configuration for all configured underlying interfaces.

Meaning The output shows the name of the underlying interface, the member links of the aggregated bundle, and the PPPoE family configuration. The output shows packet counts when traffic is present on the logical interface.

Verifying the pp0 Interface Configuration

Purpose Verify that the interface values match your configuration.

Action From operational mode, enter the **show interfaces pp0** command.

```
user@host> show interfaces pp0.100
Logical interface pp0.100 (Index 71) (SNMP ifIndex 710)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionUp, Session ID: 1,
    Session AC name: pppoe-server-1, Remote MAC address: 00:90:1a:00:18:34,
    Underlying interface: demux0.10301 (Index 70)
  Link:
    ge-5/0/3.32767
    ge-5/1/2.32767
  Input packets : 18572
  Output packets: 18572
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 0 (never), Output: 18566 (00:00:02 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls:
  Not-configured
```

```

CHAP state: Closed
PAP state: Success
Protocol inet, MTU: 1500
Flags: Sendbcst-pkt-to-re
Addresses, Flags: Is-Primary
Local: 45.63.24.1

```

Meaning This output shows information about the PPPoE logical interface created on the underlying VLAN demux interface. The output includes the PPPoE family and aggregated Ethernet redundant link information, and shows input and output traffic for the PPPoE interface.

Verifying the ANCP Agent Configuration

Purpose Verify that the ANCP values match your configuration and that traffic is flowing.

Action From operational mode, enter the **show ancp subscriber** command.

```

user@host> show ancp subscriber detail
Interface  State           Last change  Primary    Secondary  Current status
ae0        On primary      ge-1/0/1    ge-1/0/2   both up

```

From operational mode, enter the **show ancp cos** command.

```

user@host> show ancp cos

Qos Adjust Flag:      TRUE
Keepalive Timer:      30 secs
Cos State:            WRITE_READY
Connect Time:         Mon Mar 19 15:03:01 2012
Session Time:         Mon Mar 19 15:03:13 2012
Routing Instance Time: Mon Mar 19 15:03:14 2012
Keepalive Time:       Not Set
Rate Update Time:     Mon Mar 19 15:03:15 2012

```

Type	Name	Index	Pending Update	Last Update
iflset	10301	1	None	64 Kbps
iflset	10302	2	None	64 Kbps
iflset	10303	71	None	64 Kbps

Meaning The **show ancp subscriber** output shows subscriber line information such as state and the various traffic rates collected by the ANCP agent—displayed for each subscriber as identified by the ACI. The **show ancp cos** output shows that the ANCP agent is configured to send adjusted rate data to CoS, that keepalives are configured for a 30-second interval, and that the interface sets 10301, 10302, and 10303 are configured and their traffic rates are updating

Related Documentation

- [Dynamic Profiles Overview](#)
- [Configuring a Dynamic Profile for Client Access](#)
- [Subscriber Interfaces and Demultiplexing Overview](#)
- [ANCP Agent Interactions with AAA on page 13](#)
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 23](#)

- [Configuring the ANCP Agent on page 29](#)
- *AAA Service Framework Overview*

CHAPTER 5

Configuration Statements

- [\[edit protocols ancp\] Hierarchy Level](#) on page 66
- [access-identifier](#) on page 67
- [adjacency-timer](#) on page 68
- [advisory-options \(Traffic Shaping\)](#) on page 69
- [ancp](#) on page 70
- [ancp-speed-change-immediate-update \(ANCP\)](#) on page 71
- [downstream-rate \(Traffic Shaping\)](#) on page 72
- [exclude \(RADIUS\)](#) on page 73
- [gsmp-syn-timeout \(ANCP\)](#) on page 77
- [gsmp-syn-wait \(ANCP\)](#) on page 78
- [ietf-mode](#) on page 78
- [interface-set \(ANCP\)](#) on page 79
- [interfaces \(ANCP\)](#) on page 80
- [juniper-dsl-attributes](#) on page 81
- [maximum-discovery-table-entries](#) on page 82
- [maximum-helper-restart-time](#) on page 82
- [neighbor \(Define ANCP\)](#) on page 83
- [overhead-accounting \(ANCP\)](#) on page 84
- [pre-ietf-mode](#) on page 85
- [qos-adjust](#) on page 85
- [qos-adjust-adsl](#) on page 86
- [qos-adjust-adsl2](#) on page 86
- [qos-adjust-adsl2-plus](#) on page 87
- [qos-adjust-sdsl](#) on page 87
- [qos-adjust-vdsl](#) on page 88
- [qos-adjust-vdsl2](#) on page 88
- [traceoptions \(ANCP\)](#) on page 89

- [underlying-interface \(ANCP\)](#) on page 91
- [upstream-rate \(Traffic Shaping\)](#) on page 92

[\[edit protocols ancp\]](#) Hierarchy Level

```
protocols {
  ancp {
    adjacency-timer seconds;
    gsmp-syn-timeout seconds;
    gsmp-syn-wait;
    interfaces {
      interface-set interface-set-name {
        access-identifier identifier-string;
        underlying-interface underlying-interface-name;
      }
      interface-name {
        access-identifier identifier-string;
      }
    }
    maximum-discovery-table-entries entry-number;
    maximum-helper-restart-time;
    neighbor ip-address {
      adjacency-timer;
      ietf-mode;
      maximum-discovery-table-entries entry-number;
      pre-ietf-mode;
    }
    pre-ietf-mode;
    qos-adjust;
    qos-adjust-adsl adjustment-factor;
    qos-adjust-adsl2 adjustment-factor;
    qos-adjust-adsl2-plus adjustment-factor;
    qos-adjust-sds1 adjustment-factor;
    qos-adjust-vds1 adjustment-factor;
    qos-adjust-vds2 adjustment-factor;
    traceoptions {
      file filename <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
      flag flag;
      level (all | error | info | notice | verbose | warning);
      no-remote-trace;
    }
  }
}
```

- Related Documentation**
- [ANCP and the ANCP Agent Overview](#) on page 3
 - [Configuring the ANCP Agent](#) on page 29

access-identifier

Syntax	<code>access-identifier <i>identifier-string</i>;</code>
Hierarchy Level	[edit protocols ancp interfaces <i>interface-name</i>], [edit protocols ancp interfaces interface-set]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Associate an access-loop circuit identifier (ACI) with the VLAN or set of VLANs that carry traffic to the subscriber using that access loop; identify a particular subscriber. This statement requires that the name of the interface or interface set is statically configured or deterministic. This means that it can be used with dynamic or static interface sets, VLAN-tagged interface sets, or static VLAN/VLAN demux interfaces.
Options	<i>identifier-string</i> —Unique identifier string for the access loop circuit; also configured on the access node.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Associating an Access Node with Subscribers for ANCP Agent Operations on page 32

adjacency-timer

Syntax	adjacency-timer <i>seconds</i> ;
Hierarchy Level	[edit protocols ancp], [edit protocols ancp neighbor ip-address]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Specify a value for the interval that the ANCP agent proposes during negotiation to establish an adjacency, for all neighbors or a specific neighbor. The larger of the values proposed by the agent and the neighbor is selected for the interval between subsequent adjacency messages exchanged by the agent and the neighbor.
Options	seconds —Number of seconds between adjacency messages. Range: 1 through 25 seconds Default: 10 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Specifying the Interval Between ANCP Adjacency Messages on page 33• Configuring ANCP Neighbors on page 31

advisory-options (Traffic Shaping)

Syntax	<pre>advisory-options { downstream-rate rate; upstream-rate rate; }</pre>
Hierarchy Level	<p>[edit dynamic-profiles <i>profile-name</i> interfaces \$junos-interface-ifd-name unit \$junos-interface-unit],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces interface-set \$junos-interface-set-name interface \$junos-interface-ifd-name],</p> <p>[edit interfaces demux0 unit <i>logical-unit-number</i>],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Support at the [edit interfaces demux0 ...] hierarchy level introduced in Junos OS Release 12.2.</p> <p>Support at the [edit dynamic-profiles ...] hierarchy level introduced in Junos OS Release 13.1.</p>
Description	<p>Specify a recommended shaping rate to be applied to downstream or upstream traffic on an interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 38 • Configuring the ANCP Agent on page 29 • Configuring the Method to Set the LAC Connection Speeds to the LNS

ancp

```
Syntax  ancp {
        adjacency-timer seconds;
        gsmp-syn-timeout seconds;
        gsmp-syn-wait;
        interfaces {
            interface-set interface-set-name {
                access-identifier identifier-string;
                underlying-interface underlying-interface-name;
            }
            interface-name {
                access-identifier identifier-string;
            }
        }
        maximum-discovery-table-entries entry-number;
        maximum-helper-restart-time;
        neighbor ip-address {
            adjacency-timer;
            ietf-mode;
            maximum-discovery-table-entries entry-number;
            pre-ietf-mode;
        }
        pre-ietf-mode;
        qos-adjust;
        qos-adjust-adsl adjustment-factor;
        qos-adjust-adsl2 adjustment-factor;
        qos-adjust-adsl2-plus adjustment-factor;
        qos-adjust-sdsl adjustment-factor;
        qos-adjust-vdsl adjustment-factor;
        qos-adjust-vdsl2 adjustment-factor;
        traceoptions {
            file filename <files number> <match regular-expression > <size maximum-file-size>
                <world-readable | no-world-readable>;
            flag flag;
            level (all | error | info | notice | verbose | warning);
            no-remote-trace;
        }
    }
```

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 9.4.

Description Configure Junos OS ANCP agent features.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- [Configuring the ANCP Agent on page 29](#)

ancp-speed-change-immediate-update (ANCP)

Syntax	ancp-speed-change-immediate-update;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Configure AAA to generate immediate interim accounting updates to the RADIUS server in response to ANCP agent notifications of rate changes on subscriber access lines.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications on page 41• Configuring Per-Subscriber Session Accounting• Configuring the ANCP Agent on page 29

downstream-rate (Traffic Shaping)

Syntax	<code>downstream-rate rate;</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> interfaces \$junos-interface-ifd-name unit \$junos-interface-unit advisory-options],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces interface-set \$junos-interface-set-name interface \$junos-interface-ifd-name advisory-options],</code> <code>[edit interfaces demux0 unit <i>logical-unit-number</i> advisory-options],</code> <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> advisory-options]</code>
Release Information	Statement introduced in Junos OS Release 11.4. Support at the <code>[edit interfaces demux0 ...]</code> hierarchy level introduced in Junos OS Release 12.2. Support at the <code>[edit dynamic-profiles ...]</code> hierarchy level introduced in Junos OS Release 13.1.
Description	<p>Specify a recommended shaping rate to be applied to downstream traffic on an interface.</p> <p>For ANCP interfaces, this configured rate is used as the default value for the Juniper VSA Downstream-Calculated-Qos-Rate (26–141) when the router has not received and processed the attributes from the access node.</p> <p>For L2TP, the rate is configured on an underlying PPPoE logical interface for a subscriber on an MX Series router acting as a LAC. When the subscriber is tunneled, this rate, referred to as speed for L2TP, is sent to the LNS in the ICCN message as AVP 24.</p>
Options	<p>rate—Traffic rate in bits per second.</p> <p>Range: 1000 through 4,294,967,295 bits per second</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 38• Configuring the ANCP Agent on page 29• Configuring the Method to Set the LAC Connection Speeds to the LNS

exclude (RADIUS)

```
Syntax  exclude {
    acc-aggr-cir-id-asc [ access-request | accounting-start | accounting-stop ];
    acc-aggr-cir-id-bin [ access-request | accounting-start | accounting-stop ];
    acc-loop-cir-id [ access-request | accounting-start | accounting-stop ];
    accounting-authentic [ accounting-on | accounting-off ];
    accounting-delay-time [ accounting-on | accounting-off ];
    accounting-session-id [ access-request | accounting-on | accounting-off | accounting-stop
    ];
    accounting-terminate-cause [ accounting-off ];
    act-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    act-data-rate-up [ access-request | accounting-start | accounting-stop ];
    act-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
    act-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
    att-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    att-data-rate-up [ access-request | accounting-start | accounting-stop ];
    called-station-id [ access-request | accounting-start | accounting-stop ];
    calling-station-id [ access-request | accounting-start | accounting-stop ];
    class [ accounting-start | accounting-stop ];
    cos-shaping-rate [ accounting-start | accounting-stop ];
    dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
    dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
    dhcp-options [ access-request | accounting-start | accounting-stop ];
    downstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop
    ];
    dsl-forum-attributes [ access-request | accounting-start | accounting-stop ];
    dsl-line-state [ access-request | accounting-start | accounting-stop ];
    dsl-type [ access-request | accounting-start | accounting-stop ];
    event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop
    ];
    filter-id [ accounting-start | accounting-stop ];
    framed-ip-address [ accounting-start | accounting-stop ];
    framed-ip-netmask [ accounting-start | accounting-stop ];
    input-filter [ accounting-start | accounting-stop ];
    input-gigapackets [ accounting-stop ];
    input-gigawords [ accounting-stop ];
    interface-description [ access-request | accounting-start | accounting-stop ];
    max-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    max-data-rate-up [ access-request | accounting-start | accounting-stop ];
    max-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
    max-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
    min-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    min-data-rate-up [ access-request | accounting-start | accounting-stop ];
    min-lp-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    min-lp-data-rate-up [ access-request | accounting-start | accounting-stop ];
    nas-identifier [ access-request | accounting-on | accounting-off | accounting-start |
    accounting-stop ];
    nas-port [ access-request | accounting-start | accounting-stop ];
    nas-port-id [ access-request | accounting-start | accounting-stop ];
    nas-port-type [ access-request | accounting-start | accounting-stop ];
    output-filter [ accounting-start | accounting-stop ];
    output-gigapackets [ accounting-stop ];
    output-gigawords [ accounting-stop ];
```

```
    upstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop ];  
}
```

Hierarchy Level [edit access profile *profile-name* radius attributes]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Options **downstream-calculated-qos-rate**, **dsl-forum-attributes**, and
upstream-calculated-qos-rate introduced in Junos OS Release 11.4.
Options **cos-shaping-rate** and **filter-id** introduced in Junos OS Release 13.2.

Description Configure the router or switch to exclude the specified attributes from the specified type of RADIUS message.

Not all attributes are available in all types of RADIUS messages. By default, the router or switch includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages.

Options RADIUS attribute type—RADIUS attribute, Juniper Networks (vendor ID 4874) VSA number and name, or DSL Forum (vendor ID 3561) VSA number and name.

- **acc-aggr-cir-id-asc**—Juniper Networks VSA 26-112, Acc-Aggr-Cir-Id-Asc.
- **acc-aggr-cir-id-bin**—Juniper Networks VSA 26-111, Acc-Aggr-Cir-Id-Bin.
- **acc-loop-cir-id**—Juniper Networks VSA 26-110, Acc-Loop-Cir-Id.
- **accounting-authentic**—RADIUS attribute 45, Acct-Authentic.
- **accounting-delay-time**—RADIUS attribute 41, Acct-Delay-Time.
- **accounting-session-id**—RADIUS attribute 44, Acct-Session-Id.
- **accounting-terminate-cause**—RADIUS attribute 49, Acct-Terminate-Cause.
- **act-data-rate-dn**—Juniper Networks VSA 26-114, Act-Data-Rate-Dn
- **act-data-rate-up**—Juniper Networks VSA 26-113, Act-Data-Rate-Up
- **act-interlv-delay-dn**—Juniper Networks VSA 26-126, Act-Interlv-Delay-Dn
- **act-interlv-delay-up**—Juniper Networks VSA 26-124, Act-Interlv-Delay-Up
- **att-data-rate-dn**—Juniper Networks VSA 26-118, Att-Data-Rate-Dn
- **att-data-rate-up**—Juniper Networks VSA 26-117, Att-Data-Rate-Up
- **called-station-id**—RADIUS attribute 30, Called-Station-Id.
- **calling-station-id**—RADIUS attribute 31, Calling-Station-Id.
- **class**—RADIUS attribute 25, Class.
- **cos-shaping-rate**—Juniper Networks VSA 26-177, Cos-Shaping-Rate.
- **dhcp-gi-address**—Juniper Networks VSA 26-57, DHCP-GI-Address.
- **dhcp-mac-address**—Juniper Networks VSA 26-56, DHCP-MAC-Address.
- **dhcp-options**—Juniper Networks VSA 26-55, DHCP-Options.
- **downstream-calculated-qos-rate**—Juniper Networks VSA 26-141
- **dsl-forum-attributes**—DSL Forum VSA (vendor ID 3561) as described in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*
- **dsl-line-state**—Juniper Networks VSA 26-127, DSL-Line-State
- **dsl-type**—Juniper Networks VSA 26-128, DSL-Type
- **event-timestamp**—RADIUS attribute 55, Event-Timestamp.
- **filter-id**—RADIUS attribute 11, Filter-Id.
- **framed-ip-address**—RADIUS attribute 8, Framed-IP-Address.
- **framed-ip-netmask**—RADIUS attribute 9, Framed-IP-Netmask.
- **input-filter**—Juniper Networks VSA 26-10, Ingress-Policy-Name.
- **input-gigapackets**—Juniper Networks VSA 26-42, Acct-Input-Gigapackets.

- **input-gigawords**—RADIUS attribute 52, Acct-Input-Gigawords.
- **interface-description**—Juniper Networks VSA 26-53, Interface-Desc.
- **max-data-rate-dn**—Juniper Networks VSA 26-120, Max-Data-Rate-Dn
- **max-data-rate-up**—Juniper Networks VSA 26-119, Max-Data-Rate-Up
- **max-interlv-delay-dn**—Juniper Networks VSA 26-125, Max-Interlv-Delay-Dn
- **max-interlv-delay-up**—Juniper Networks VSA 26-123, Max-Interlv-Delay-Up
- **min-data-rate-dn**—Juniper Networks VSA 26-116, Min-Data-Rate-Dn
- **min-data-rate-up**—Juniper Networks VSA 26-115, Min-Data-Rate-Up
- **min-lp-data-rate-dn**—Juniper Networks VSA 26-122, Min-Lp-Data-Rate-Dn
- **min-lp-data-rate-up**—Juniper Networks VSA 26-121, Min-Lp-Data-Rate-Up
- **nas-identifier**—RADIUS attribute 32, NAS-Identifier.
- **nas-port**—RADIUS attribute 5, NAS-Port.
- **nas-port-id**—RADIUS attribute 87, NAS-Port-Id.
- **nas-port-type**—RADIUS attribute 61, NAS-Port-Type.
- **output-filter**—Juniper Networks VSA 26-11, Egress-Policy-Name.
- **output-gigapackets**—Juniper Networks VSA 26-43, Acct-Output-Gigapackets.
- **output-gigawords**—RADIUS attribute 53, Acct-Output-Gigawords.
- **upstream-calculated-qos-rate**—Juniper Networks VSA 26-142

RADIUS message type

- **access-request**—RADIUS Access-Accept messages.
- **accounting-off**—RADIUS Accounting-Off messages.
- **accounting-on**—RADIUS Accounting-On messages.
- **accounting-start**—RADIUS Accounting-Start messages.
- **accounting-stop**—RADIUS Accounting-Stop messages.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• <i>Configuring RADIUS Server Parameters for Subscriber Access</i>
------------------------------	---

gsmp-syn-timeout (ANCP)

Syntax	<code>gsmp-syn-timeout <i>seconds</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Configure the maximum period that the ANCP agent waits before sending a SYN message to an ANCP neighbor to negotiate the adjacency. If the neighbor sends a SYN message during this period, the ANCP agent uses the partition information in the neighbor's message when generating its own initial SYN message to the neighbor. The agent does not wait for the period to expire if it receives a SYN message from the neighbor.
Options	<i>seconds</i> —Number of seconds the ANCP agent waits. Range: 1 through 60 seconds Default: 60 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Configuring the ANCP Agent to Learn ANCP Partition IDs on page 35

gsmp-syn-wait (ANCP)

Syntax	gsmp-syn-wait;
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 13.3
Description	Enable the ANCP agent to learn partition ID information from neighbors, in support of nonzero ANCP partition IDs. This statement forces the ANCP agent to delay sending a SYN message during adjacency negotiation for a configurable period. When the neighbor sends a SYN message to the ANCP agent during that period, the agent learns the partition ID information from the neighbor and uses that information when it sends its own SYN message. If the agent does not receive the message during the period, then it sends a SYN message to the neighbor when the period times out.
Default	This statement is disabled. The ANCP agent does not wait before sending the initial SYN message and does not support nonzero partition IDs.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Configuring the ANCP Agent to Learn ANCP Partition IDs on page 35

ietf-mode

Syntax	ietf-mode
Hierarchy Level	[edit protocols ancp neighbor ip-address]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Configure the ANCP agent to run in a mode that is not backward compatible with Internet draft-wadhwa-gsmp-l2control-configuration-00.txt, <i>GSMP extensions for layer2 control (L2C)</i> . Include this statement when pre-ietf mode has been configured globally for the ANCP agent, but you want one or more neighbors to run in the default mode.
Default	ANCP does not run in a backward-compatible mode.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Configuring ANCP Neighbors on page 31

interface-set (ANCP)

Syntax	<code>interface-set <i>interface-set-name</i> { <code>access-identifier</code> <i>identifier-string</i>; <code>underlying-interface</code> <i>underlying-interface-name</i>; }</code>
Hierarchy Level	[edit protocols ancp interfaces]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Identify a group of VLANs on which traffic is sent to a subscriber identified by the access-loop circuit identifier.
Options	<p><i>interface-set-name</i>—Name of a group of VLANs that carry traffic to the subscriber identified by the access loop circuit identifier.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Associating an Access Node with Subscribers for ANCP Agent Operations on page 32

interfaces (ANCP)

Syntax	<pre>interfaces { interface-set interface-set-name { access-identifier identifier-string; underlying-interface underlying-interface-name; } interface-name { access-identifier identifier-string } }</pre>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Identify the subscribers whose traffic is reported and shaped by the ANCP agent.
Options	<p>interface-name—Name of a logical interface supporting a single VLAN that carries traffic to the subscriber identified by the access-loop circuit identifier.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Associating an Access Node with Subscribers for ANCP Agent Operations on page 32

juniper-dsl-attributes

Syntax	juniper-dsl-attributes;
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	<p>Configure AAA to add Juniper Networks DSL VSAs to the RADIUS authentication and accounting request messages for subscribers. If the router has not received and processed the corresponding ANCP attributes from the access node, then AAA provides only the following in these RADIUS messages:</p> <ul style="list-style-type: none"> Downstream-Calculated-QoS-Rate (IANA 4874, 26-141)—Default configured advisory transmit speed. Upstream-Calculated-QoS-Rate (IANA 4874, 26-142)—Default configured advisory receive speed.
Default	The Juniper Networks DSL VSAs are not added to the RADIUS authentication and accounting request messages. However, the DSL Forum VSA—if available—is added to RADIUS messages by default.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 40 Configuring the ANCP Agent on page 29

maximum-discovery-table-entries

Syntax	<code>maximum-discovery-table-entries <i>entry-number</i>;</code>
Hierarchy Level	[edit protocols ancp], [edit protocols ancp neighbor ip-address]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Specify the maximum number of discovery table entries accepted from all ANCP neighbors or from a particular ANCP neighbor. The number of entries configured for an individual neighbor supersedes the global value. The neighbor can continue to update previously created entries when the maximum has been exceeded, but no new entries are accepted.
Default	No limit on the number of table entries
Options	<i>entry-number</i> —Maximum number of discovery table entries. Range: 1 through 100,000 Default: 100,000
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Configuring ANCP Neighbors on page 31


maximum-helper-restart-time

Syntax	<code>maximum-helper-restart-time <i>seconds</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Specify how long other router processes wait for the ANCP agent to restart before considering it to be down.
Options	<i>seconds</i> —Number of seconds other processes wait for ANCP to restart. Range: 45 through 600 seconds Default: 45 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Specifying How Long Processes Wait for the ANCP Agent Restart to Complete on page 35

neighbor (Define ANCP)

Syntax	<pre>neighbor <i>ip-address</i> { adjacency-timer <i>seconds</i>; ietf-mode; maximum-discovery-table-entries; pre-ietf-mode; }</pre>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Configure an ANCP neighbor with which the ANCP agent on the router forms an adjacency for reporting and shaping traffic.
Options	<p><i>ip-address</i>—IP address of the ANCP neighbor.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Configuring ANCP Neighbors on page 31

overhead-accounting (ANCP)

Syntax	overhead-accounting;
Hierarchy Level	[edit protocols ancp interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	<p>Prevent ANCP from performing an adjustment on the actual downstream data rate that ANCP receives from the DSLAM for the difference between the customer premise equipment (CPE) protocol overhead and the B-RAS protocol overhead. You include this statement when you want CoS to perform the adjustment on the data rate from the DSLAM according to the overhead accounting configuration in a CoS traffic control profile.</p> <p>When this statement is not configured (the default condition), ANCP makes the traffic rate adjustment according to the configuration of the qos-adjust-line-type statements and reports that rate to CoS. CoS then applies (if configured) the adjustment set by the overhead-accounting statement in the CoS traffic profile.</p>
	<div> NOTE: ANCP reports a traffic rate to CoS only if the qos-adjust statement at the [edit protocols ancp] hierarchy level has been configured.</div>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29

pre-ietf-mode

Syntax	pre-ietf-mode
Hierarchy Level	[edit protocols ancp], [edit protocols ancp neighbor ip-address]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Configure the ANCP agent to run in a mode that is backward compatible with Internet draft draft-wadhwa-gsmp-l2control-configuration-00.txt, <i>GSMP extensions for layer2 control (L2C)</i> for all neighbors or for a specific neighbor.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the ANCP Agent on page 29 • Configuring the ANCP Agent for Backward Compatibility on page 34 • Configuring ANCP Neighbors on page 31

qos-adjust

Syntax	qos-adjust;
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Specify that the ANCP agent reports net data rates for downstream traffic to CoS. When this statement is not configured, ANCP does not report traffic rates to CoS.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the ANCP Agent to Report Traffic Rates to CoS on page 37 • Traffic Rate Reporting and Adjustment by the ANCP Agent on page 10 • Configuring the ANCP Agent on page 29

qos-adjust-adsl

Syntax	<code>qos-adjust-adsl <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an ADSL line. The ANCP agent reports the adjusted rate only to AAA.
Options	<i>adjustment-factor</i> —Adjustment factor applied to upstream and downstream data rates for the DSL type. Range: 0 through 100 percent Default: 100 percent
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 36• Configuring the ANCP Agent on page 29

qos-adjust-adsl2

Syntax	<code>qos-adjust-adsl2 <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an ADSL2 line. The ANCP agent reports the adjusted rate only to AAA.
Options	<i>adjustment-factor</i> —Adjustment factor applied to upstream and downstream data rates for the DSL type. Range: 0 through 100 percent Default: 100 percent
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 36• Configuring the ANCP Agent on page 29

qos-adjust-adsl2-plus

Syntax	<code>qos-adjust-adsl2-plus <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an ADSL2+ line. The ANCP agent reports the adjusted rate only to AAA.
Options	<p><i>adjustment-factor</i>—Adjustment factor applied to upstream and downstream data rates for the DSL type.</p> <p>Range: 0 through 100 percent</p> <p>Default: 100 percent</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 36 • Configuring the ANCP Agent on page 29

qos-adjust-sdsl

Syntax	<code>qos-adjust-sdsl <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an SDS1 line. The ANCP agent reports the adjusted rate only to AAA.
Options	<p><i>adjustment-factor</i>—Adjustment factor applied to upstream and downstream data rates for the DSL type.</p> <p>Range: 0 through 100 percent</p> <p>Default: 100 percent</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 36 • Configuring the ANCP Agent on page 29

qos-adjust-vds1

Syntax	<code>qos-adjust-vds1 <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an VDS1 line. The ANCP agent reports the adjusted rate only to AAA.
Options	<i>adjustment-factor</i> —Adjustment factor applied to upstream and downstream data rates for the DSL type. Range: 0 through 100 percent Default: 100 percent
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 36• Configuring the ANCP Agent on page 29

qos-adjust-vds2

Syntax	<code>qos-adjust-vds2 <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an VDS2 line. The ANCP agent reports the adjusted rate only to AAA.
Options	<i>adjustment-factor</i> —Adjustment factor applied to upstream and downstream data rates for the DSL type. Range: 0 through 100 percent Default: 100 percent
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 36• Configuring the ANCP Agent on page 29

traceoptions (ANCP)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i> <disable>; level (all error info notice verbose warning); no-remote-trace; } </pre>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Define tracing operations for ANCP agent processes.
Options	<p>file <i>filename</i>— Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. Include the disable option after a flag to disable tracing for that flag. You can include the following flags:</p> <ul style="list-style-type: none"> • all—Trace all operations. • config—Trace configuration events. • cos—Trace class-of-service events. • general—Trace general flow. • packet—Trace ANCP packet transmit and receive operations. • process—Trace process internals. • protocol—Trace protocol events. • restart—Trace process restart flow • routing-socket—Trace routing socket events. • session—Trace connection events and flow. • startup—Trace ANCP startup events and flow. • subscriber—Trace subscriber events. • timer—Trace timer processing. <p>level—Level of tracing to perform. You can specify any of the following levels:</p>

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Tracing ANCP Agent Operations for Subscriber Access on page 137
------------------------------	---

underlying-interface (ANCP)

Syntax	<code>underlying-interface <i>underlying-interface-name</i>;</code>
Hierarchy Level	[edit protocols ancp interfaces interface-set <i>interface-set-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure the underlying interface on which the VLAN demux interface is running. The VLAN demux interface is the underlying interface for the PPPoE sessions controlled by ANCP.
Options	<i>underlying-interface-name</i> —Name of the underlying interface.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 29• Associating an Access Node with Subscribers for ANCP Agent Operations on page 32

upstream-rate (Traffic Shaping)

Syntax	<code>upstream-rate rate;</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> interfaces \$junos-interface-ifd-name unit \$junos-interface-unit advisory-options],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces interface-set \$junos-interface-set-name interface \$junos-interface-ifd-name advisory-options],</code> <code>[edit interfaces demux0 unit <i>logical-unit-number</i> advisory-options],</code> <code>[edit interfaces <i>interface-name</i> <i>logical-unit-number</i> advisory-options]</code>
Release Information	Statement introduced in Junos OS Release 11.4. Support at the <code>[edit interfaces demux0 ...]</code> hierarchy level introduced in Junos OS Release 12.2. Support at the <code>[edit dynamic-profiles ...]</code> hierarchy level introduced in Junos OS Release 13.1.
Description	<p>Specify a recommended shaping rate to be applied to upstream traffic on an interface.</p> <p>For ANCP interfaces, this configured rate is used as the default value for the Juniper VSA Upstream-Calculated-Qos-Rate (26-142) when the router has not received and processed the attributes from the access node.</p> <p>For L2TP, the rate is configured on an underlying PPPoE logical interface for a subscriber on an MX Series router acting as a LAC. When the subscriber is tunneled, this rate, referred to as speed for L2TP, is sent to the LNS in the ICCN message as AVP 38.</p>
Options	rate —Traffic rate in bits per second. Range: 1000 through 4,294,967,295 bits per second
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 38• Configuring the ANCP Agent on page 29• Configuring the Method to Set the LAC Connection Speeds to the LNS

PART 3

Administration

- [Monitoring ANCP for Subscriber Access on page 95](#)
- [Monitoring Commands on page 99](#)

CHAPTER 6

Monitoring ANCP for Subscriber Access

- [Verifying and Monitoring ANCP Neighbors on page 95](#)
- [Clearing ANCP Neighbors on page 96](#)
- [Verifying and Monitoring ANCP Subscribers on page 96](#)
- [Clearing ANCP Subscribers on page 97](#)
- [Verifying and Monitoring CoS for ANCP Subscribers on page 97](#)
- [Clearing and Verifying ANCP Statistics on page 97](#)

Verifying and Monitoring ANCP Neighbors

Purpose View ANCP neighbor information:

Action • To display summary information about all ANCP neighbors:

user@host> [show ancp neighbor](#)

- To display information about a specific ANCP neighbor, add the IP address or MAC address to the command:

user@host> [show ancp neighbor 10.25.64.21](#)

- To display detailed information, add **detail** to the command:

user@host> [show ancp neighbor detail](#)

user@host> [show ancp neighbor ba:ad:be:ef:10:10 detail](#)

- To display a count of ANCP neighbors in various states and the total number of neighbors, or a count of DSL lines in various states for all subscribers for a particular neighbor:

user@host> [show ancp summary neighbor](#)

user@host> [show ancp summary neighbor 10.25.64.21](#)

- To display total and state-wise counts of both ANCP neighbors and subscribers:

user@host> [show ancp summary](#)

Related Documentation • [CLI Explorer](#)

Clearing ANCP Neighbors

Purpose Clear ANCP neighbor information.

- Action**
- To clear connections with all ANCP neighbors:
user@host> `clear ancp neighbor`
 - To clear the connection with a specific ANCP neighbor, add the IP address or MAC address to the command:
user@host> `clear ancp neighbor ip-address 10.25.64.21`
user@host> `clear ancp neighbor system-name ba:ad:be:ef:10:10`
 - To verify that the connection has been cleared:
user@host> `show ancp neighbor`
user@host> `show ancp neighbor 10.25.64.21`
user@host> `show ancp neighbor ba:ad:be:ef:10:10`

Related Documentation

- [CLI Explorer](#)

Verifying and Monitoring ANCP Subscribers

Purpose View ANCP subscriber (local access loop) information:

- Action**
- To display summary information about all ANCP subscribers:
user@host> `show ancp subscriber`
 - To display information about all ANCP subscribers connected through a particular ANCP neighbor:
user@host> `show ancp subscriber neighbor 10.25.64.21`
 - To display information about an ANCP subscriber specified by the ACI:
user@host> `show ancp subscriber "port-2-11"`
 - To display detailed information, add **detail** to the command:
user@host> `show ancp subscriber detail`
user@host> `show ancp subscriber neighbor 10.25.64.21 detail`
 - To display a count of subscribers in various states and the total number of subscribers:
user@host> `show ancp summary subscriber`
 - To display total and state-wise counts of both ANCP neighbors and subscribers:
user@host> `show ancp summary`

Related Documentation

- [CLI Explorer](#)

Clearing ANCP Subscribers

Purpose Clear ANCP subscriber information.

- Action**
- To clear connections with all ANCP subscribers:

```
user@host> clear ancp subscriber
```
 - To clear the connection with an ANCP subscriber identified by a particular ACI on all neighbors, add the identifier to the command:

```
user@host> clear ancp subscriber identifier port-2-10
```
 - To clear the connection with an ANCP subscriber identified by a particular ACI on a specific neighbor, add the identifier and either the IP address or MAC address to the command:

```
user@host> clear ancp subscriber identifier port-2-10 ip-address 10.25.64.21
```

```
user@host> clear ancp subscriber identifier port-2-10 system-name ba:ad:be:ef:10:10
```
 - To verify that the connection has been cleared:

```
user@host> show ancp subscriber
```

Related Documentation

- [CLI Explorer](#)

Verifying and Monitoring CoS for ANCP Subscribers

Purpose View ANCP CoS state information:

- Action**
- To display summary information about the CoS state for all ANCP subscribers:

```
user@host> show ancp cos
```
 - To display information about the CoS state for an ANCP subscriber specified by the ACI:

```
user@host> show ancp cos "port-2-11"
```
 - To display the most recently updated CoS information:

```
user@host> show ancp cos last-update
```
 - To display the CoS information that is pending (will be used to update the fields):

```
user@host> show ancp cos pending-update
```

Related Documentation

- [CLI Explorer](#)

Clearing and Verifying ANCP Statistics

Purpose Clear ANCP statistics.

- Action**
- To clear all ANCP statistics:

user@host> **clear ancp statistics**

- To clear statistics for a specific ANCP neighbor, add the IP address or MAC address to the command:

user@host> **clear ancp statistics ip-address 10.25.64.21**

user@host> **clear ancp statistics system-name ba:ad:be:ef:10:10**

- To verify that the connection has been cleared:

user@host> **show ancp neighbor**

**Related
Documentation**

- [ANCP and the ANCP Agent Overview on page 3](#)

CHAPTER 7

Monitoring Commands

- `clear ancp neighbor`
- `clear ancp statistics`
- `clear ancp subscriber`
- `request ancp oam interface`
- `request ancp oam neighbor`
- `show ancp cos`
- `show ancp neighbor`
- `show ancp statistics`
- `show ancp subscriber`
- `show ancp summary`
- `show ancp summary neighbor`
- `show ancp summary subscriber`

clear ancp neighbor

Syntax	clear ancp neighbor <ip-address <i>ip-address</i>> <system-name <i>mac-address</i>>
Release Information	Command introduced in Junos OS Release 9.4.
Description	Clear the ANCP agent connection with all ANCP neighbors or with the specified ANCP neighbor. This command deletes information for subscribers associated with the neighbor, causing the adjusted traffic rates to revert to the configured rate for the subscriber interfaces. The neighbor remains configured (its administrative state is <i>enabled</i>) and can reestablish adjacencies.
Options	none —Clear all ANCP neighbors. ip-address <i>ip-address</i> —(Optional) Clear the ANCP neighbor specified by the IP address. system-name <i>mac-address</i> —(Optional) Clear the ANCP neighbor specified by the MAC address.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show ancp neighbor on page 111
List of Sample Output	clear ancp neighbor on page 100 show ancp neighbor on page 100
Output Fields	When you enter this command, you are provided no feedback on the status of your request. You can enter the show ancp neighbor command before and after clearing the ANCP neighbors to verify the clear operation.

Sample Output

clear ancp neighbor

```
user@host> clear ancp neighbor
```

show ancp neighbor

The following sample output displays the connections with ANCP neighbors before and after the **clear ancp neighbor** command was issued.

```
user@host> show ancp neighbor
```

IP Address	MAC Address	State	Subscriber Count	Capabilities
10.10.10.2	ba:ad:be:ef:10:10	Established	5	Topo
12.12.12.2	ba:ad:be:ef:10:12	Established	5	Topo
13.13.13.2	ba:ad:be:ef:10:13	Established	5	Topo

14.14.14.2	ba:ad:be:ef:10:14	Established	5	Topo
------------	-------------------	-------------	---	------

```
user@host> clear ancp neighbor ip-address 10.10.10.2
```

```
user@host> show ancp neighbor
```

IP Address	MAC Address	State	Subscriber Count	Capabilities
12.12.12.2	ba:ad:be:ef:10:12	Established	5	Topo
13.13.13.2	ba:ad:be:ef:10:13	Established	5	Topo
14.14.14.2	ba:ad:be:ef:10:14	Established	5	Topo

clear ancp statistics

Syntax	clear ancp statistics <ip-address <i>ip-address</i>> <system-name <i>mac-address</i>>
Release Information	Command introduced in Junos OS Release 13.3.
Description	Clear current statistics accumulated by the ANCP agent for all ANCP neighbors or the specified neighbor.
Options	none —Clear all ANCP statistics. ip-address <i>ip-address</i> —(Optional) Clear statistics for the ANCP neighbor specified by the IP address. system-name <i>mac-address</i> —(Optional) Clear statistics for the ANCP neighbor specified by the MAC address.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show ancp neighbor on page 111
List of Sample Output	clear ancp statistics on page 102 show ancp neighbor on page 102
Output Fields	When you enter this command, you are provided no feedback on the status of your request. You can enter the show ancp neighbor command before and after clearing the ANCP neighbor statistics to verify the clear operation.

Sample Output

clear ancp statistics

```
user@host> clear ancp statistics
```

show ancp neighbor

The following sample output displays statistics for an ANCP neighbor before and after the **clear ancp statistics** command was issued.

```
user@host> show ancp neighbor ip-address 192.168.10.1 detail
Neighbor Information
  IP Address           : 192.168.10.1
  System Name          : 00:00:64:1b:01:02
  Up Time               : 38
  TCP Port              : 64959
  State                 : Established
  Subscriber Count      : 7
  Capabilities          : Topology Discovery
  System Instance       : 11
```

```

Peer Instance                : 1
Adjacency Timer (in 100ms)   : 50
Peer Adjacency Timer (in 100ms) : 100
Partition Type               : 0
Partition Flag               : 1
Partition Identifier         : 0
Dead Timer                   : 22
Received Syn Count           : 47
Received Synack Count        : 48
Received Rstack Count        : 2
Received Ack Count           : 12
Received Port Up Count       : 8
Received Port Down Count     : 2
Received Other Count         : 0
Sent Syn Count               : 48
Sent Synack Count            : 47
Sent Rstack Count            : 1
Sent Ack Count               : 12
Max Discovery Limit Exceed Count : 0

```

```
user@host> clear ancp statistics ip-address 192.168.10.1
```

```
user@host> show ancp neighbor ip-address 192.168.10.1 detail
```

Neighbor Information

```

IP Address                  : 192.168.10.1
System Name                 : 00:00:64:1b:01:02
Up Time                     : 38
TCP Port                    : 64959
State                       : Established
Subscriber Count            : 7
Capabilities                 : Topology Discovery
System Instance             : 11
Peer Instance               : 1
Adjacency Timer (in 100ms)  : 50
Peer Adjacency Timer (in 100ms) : 100
Partition Type              : 0
Partition Flag              : 1
Partition Identifier         : 0
Dead Timer                  : 22
Received Syn Count          : 0
Received Synack Count       : 0
Received Rstack Count       : 0
Received Ack Count          : 0
Received Port Up Count      : 0
Received Port Down Count    : 0
Received Other Count        : 0
Sent Syn Count              : 0
Sent Synack Count           : 0
Sent Rstack Count           : 0
Sent Ack Count              : 0
Max Discovery Limit Exceed Count : 0

```

clear ancp subscriber

Syntax	<code>clear ancp subscriber</code> <code><identifier <i>identifier-string</i>></code> <code><ip-address <i>ip-address</i>></code> <code>system-name <i>mac-address</i>></code>
Release Information	Command introduced in Junos OS Release 11.4.
Description	Clear the ANCP agent connection with all ANCP subscribers or with the specified ANCP subscriber. This command deletes information for the subscribers, causing the adjusted traffic rate to revert to the configured rate for the subscriber interface, but otherwise has no affect on ANCP neighbors.
Options	<p>none—Clear all ANCP subscribers.</p> <p>identifier <i>identifier-string</i>—(Optional) Clear the ANCP subscriber identified by the access loop ID.</p> <p>ip-address <i>ip-address</i>—(Optional) Clear all ANCP subscribers on the neighbor specified by the IP address.</p> <p>system-name <i>mac-address</i>—(Optional) Clear all ANCP subscribers on the neighbor specified by the MAC address.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> show ancp subscriber on page 124
List of Sample Output	show ancp subscriber brief on page 104 clear ancp subscriber on page 105
Output Fields	When you enter this command, you are provided no feedback on the status of your request. You can enter the show ancp subscriber command before and after clearing the ANCP neighbors to verify the clear operation.

Sample Output

show ancp subscriber brief

```

user@host> show ancp subscriber brief
Loop Identifier      Type      Interface      Rate      Neighbor
                    Kbps
port-1-10            VDSL2     set-ge-10410   64         10.10.10.2
port-1-11            VDSL2     set-ge-10411   64         11.11.11.2
port-2-10            VDSL2     ge-1/0/4.12    64         10.12.12.2
port-2-10            VDSL2     ge-1/0/4.12    64         10.12.12.3
port-2-11            VDSL2     ge-1/0/4.13    64         10.13.13.2
user@host> clear ancp subscriber identifier port-2-10

```



```
user@host> show ancp subscriber brief
```

Loop Identifier	Type	Interface	Rate Kbps	Neighbor
port-1-10	VDSL2	set-ge-10410	64	10.10.10.2
port-1-11	VDSL2	set-ge-10411	64	11.11.11.2
port-2-11	VDSL2	ge-1/0/4.13	64	10.13.13.2

`clear ancp subscriber`

```
user@host> clear ancp subscriber
```

request ancp oam interface

Syntax	request ancp oam interface <i>(interface-name interface-set set-name)</i> <count <i>count</i> > <timeout <i>duration</i> >
Release Information	Command introduced in Junos OS Release 11.4.
Description	Trigger the access node to run a loopback test on the local loop between the access node and the customer premises equipment. You must specify either an ANCP interface or an ANCP interface set. The access node responds to the NAS with the results of the test.
Options	<p>interface-name—Name of the ANCP interface on whose local loop the loopback test is run.</p> <p>interface-set set-name—Name of the ANCP interface set on whose local loop the loopback test is run.</p> <p>count count—(Optional) Number of times a loopback message is sent on the local loop. Range: 1 through 32. Default: 1.</p> <p>timeout duration—(Optional) Period of time in seconds that the NAS waits for a response to the OAM request. Range: 0 through 255. Default: 5.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Triggering ANCP OAM to Test the Local Loop on page 41
List of Sample Output	request ancp oam interface on page 106
Output Fields	When you enter this command, you are provided feedback on the status of your request, including the result of the test, the response code, and the response string returned with the OAM response in the event of failure, an error code is displayed.

Sample Output

request ancp oam interface

```
user@host> request ancp oam interface ge-1/0/4.12 count 5 timeout 40
request succeeded
0x503 : DSL line status showtime
DEFAULT RESPONSE
```

request ancp oam neighbor

Syntax	<code>request ancp oam neighbor</code> (<code>ip-address <i>ip-address</i> system-name <i>neighbor-name</i></code>) <code>subscriber <i>identifier-string</i></code> < <code>count <i>count</i></code> > < <code>timeout <i>duration</i></code> >
Release Information	Command introduced in Junos OS Release 11.4.
Description	Trigger the access node to run a loopback test on the local loop between the access node and the customer premises equipment. You must specify both the access node and the subscriber. The access node responds to the NAS with the results of the test.
Options	<p><code>ip-address <i>ip-address</i></code>—IP address that specifies the access node on whose local loop the loopback test is run.</p> <p><code>system-name <i>neighbor-name</i></code>—System name that specifies the access node on whose local loop the loopback test is run.</p> <p><code>subscriber <i>identifier-string</i></code>—Access identifier that specifies the subscriber on whose local loop the loopback test is run.</p> <p><code>count <i>count</i></code>—(Optional) Number of times a loopback message is sent on the local loop. Range: 1 through 32. Default: 1.</p> <p><code>timeout <i>duration</i></code>—(Optional) Period of time in seconds that the NAS waits for a response to the OAM request. Range: 0 through 255. Default: 5.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Triggering ANCP OAM to Test the Local Loop on page 41
List of Sample Output	request ancp oam subscriber on page 107
Output Fields	When you enter this command, you are provided feedback on the status of your request, including the result of the test, the response code, and the response string returned with the OAM response in the event of failure, an error code is displayed.

Sample Output

request ancp oam subscriber

```
user@host> request ancp oam neighbor 10.10.10.1 subscriber "dslam port-1-11"
request succeeded
0x503 : DSL line status showtime
DEFAULT RESPONSE
```

show ancp cos

Syntax	show ancp cos <i>identifier</i> <last-update> <pending-update>
Release Information	Command introduced in Junos OS Release 9.4.
Description	Display information about the CoS state for subscriber traffic.
Options	<p>identifier <i>identifier</i>—(Optional) Display information about the local loops for the specified access identifier.</p> <p>last-update—(Optional) Display the most recently updated CoS information.</p> <p>pending-update—(Optional) Display the pending update of CoS information.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp neighbor on page 111 • show ancp subscriber on page 124
List of Sample Output	show ancp cos on page 109 show ancp cos last-update on page 109 show ancp cos pending-update on page 110
Output Fields	Table 8 on page 108 lists the output fields for the show ancp cos command. Output fields are listed in the approximate order in which they appear.

Table 8: show ancp cos Output Fields

Field Name	Field Description
QoS Adjust Flag	<p>State of QoS adjust: TRUE (configured) or FALSE (not configured).</p> <p>The adjustment factor (percentage) is displayed for each line type: ADSL, ADSL2, ADSL2+, VDSL, VDSL2, SDSL.</p>
Keepalive Timer	Interval between the keepalive messages that the ANCP agent sends to CoS.
Cos State	<p>State of the interaction between the ANCP agent and CoS:</p> <ul style="list-style-type: none"> • ANCPD_COS_CONNECT_NEEDED • ANCPD_COS_CONNECT_PENDING • ANCPD_COS_CONNECT_DONE • ANCPD_COS_SESSION_SENT • ANCPD_COS_WRITE_READY
Connect Time	Time at which the ANCP agent connected to CoS; useful for debugging.

Table 8: show ancp cos Output Fields (*continued*)

Field Name	Field Description
Session Time	Time at which the ANCP agent sent a session connect message to CoS; useful for debugging.
Routing Instance Time	Time at which the ANCP agent sent the routing instance to CoS; useful for debugging.
Keepalive Time	Time at which the last keepalive message was sent.
Update Time	Time at which the shaping rate was last updated.
Type	Subscriber access type: ifl indicates that a single VLAN carries subscriber traffic and iflset indicates that a set of VLANs carries subscriber traffic.
Name	System-wide name of the particular subscriber access.
Index	Access identifier.
Pending Update	Actual downstream data rate to be applied next to this local loop, in Kbps.
Last Update	Actual downstream data rate last applied to this local loop, in Kbps.

Sample Output

show ancp cos

```
user@host> show ancp cos
```

```

Qos Adjust Flag:      TRUE
ADSL adjustment factor: 95
ADSL2 adjustment factor: 90
ADSL2+ adjustment factor: 85
VDSL adjustment factor: 80
VDSL2 adjustment factor: 75
SDSL adjustment factor: 70
Keepalive Timer:      45 secs
Cos State:             WRITE_READY
Connect Time:          Not Set
Session Time:          Not Set
Routing Instance Time: Not Set
Keepalive Time:        Not Set
Update Time:           Not Set

```

Type	Name	Index	Pending Update	Last Update
iflset	set-ge-10410	1	None	64 Kbps
iflset	set-ge-10411	2	None	64 Kbps
ifl	ge-1/0/4.2	71	None	64 Kbps
ifl	ge-1/0/4.3	72	None	64 Kbps

show ancp cos last-update

```
user@host> show ancp cos last-update
```

```
Qos Adjust Flag:      TRUE
ADSL adjustment factor: 95
ADSL2 adjustment factor: 90
ADSL2+ adjustment factor:85
VDSL adjustment factor: 80
VDSL2 adjustment factor: 75
SDSL adjustment factor: 70
Keepalive Timer:      45 secs
Cos State:            WRITE_READY
Connect Time:         Mon Nov 17 15:03:01 2008
Session Time:         Mon Nov 17 15:03:13 2008
Routing Instance Time: Mon Nov 17 15:03:14 2008
Keepalive Time:       Wed Nov 19 15:32:14 2008
Update Time:          Mon Nov 17 15:03:15 2008
```

Type	Name	Index	Pending Update	Last Update
iflset	iflset0	1	None	64 Kbps
iflset	iflset1	2	None	64 Kbps

show ancp cos pending-update

```
user@host> show ancp cos pending-update
```

```
Qos Adjust Flag:      TRUE
ADSL adjustment factor: 95
ADSL2 adjustment factor: 90
ADSL2+ adjustment factor:85
VDSL adjustment factor: 80
VDSL2 adjustment factor: 75
SDSL adjustment factor: 70
Keepalive Timer:      45 secs
Cos State:            WRITE_READY
Connect Time:         Not Set
Session Time:         Not Set
Routing Instance Time: Not Set
Keepalive Time:       Not Set
Update Time:          Not Set
Keepalive Timer:      45 secs
Connect Time:         Mon Nov 17 15:03:01 2008
Session Time:         Mon Nov 17 15:03:13 2008
Routing Instance Time: Mon Nov 17 15:03:14 2008
Keepalive Time:       Wed Nov 19 15:32:29 2008
Rate Update Time:     Mon Nov 17 15:03:15 2008
```

show ancp neighbor

Syntax	show ancp neighbor <brief detail> <ip-address ip-address> <system-name mac-address>
Release Information	Command introduced in Junos OS Release 9.4.
Description	Display information about all ANCP neighbors or the specified ANCP neighbor, regardless of operational state.
Options	brief detail—(Optional) Display the specified level of detail. ip-address ip-address—(Optional) IP address of the ANCP neighbor (access node). system-name mac-address—(Optional) MAC address of the ANCP neighbor (access node).
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show ancp cos on page 108• show ancp subscriber on page 124
List of Sample Output	show ancp neighbor on page 114 show ancp neighbor detail on page 114 show ancp neighbor ip-address on page 116 show ancp neighbor system-name on page 117
Output Fields	Table 9 on page 111 lists the output fields for the show ancp neighbor command. Output fields are listed in the approximate order in which they appear.

Table 9: show ancp neighbor Output Fields

Field Name	Field Description	Level of Output
Version	Version of the ANCP implementation: <ul style="list-style-type: none">• 0x31—General Switch Management Protocol (GSMP) version 3, sub-version 1; ANCP version before <i>RFC 6320, Protocol for Access Node Control Mechanism in Broadband Networks</i>.• 0x32—ANCP version 1, defined in <i>RFC 6320, Protocol for Access Node Control Mechanism in Broadband Networks</i>.	brief detail none
IP Address	IP address of the ANCP neighbor.	brief detail none
System Name	MAC address of the ANCP neighbor.	detail

Table 9: show ancp neighbor Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	Operational state of the ANCP adjacency: <ul style="list-style-type: none"> Configured—The neighbor has been configured, but has never been in the Established state. An asterisk (*) is prefixed to the neighbor entry for this state. Establishing—Adjacency negotiations are in progress for the neighbor. An asterisk (*) is prefixed to the neighbor entry for this state. This state is rarely seen because the adjacency is established so quickly. Established—Adjacency negotiations have succeeded for the neighbor and an ANCP session has been established. Not Estblshed—Not Established; adjacency negotiations are ready to begin. Indicates that this neighbor previously had been in the Established state; that is, it has lost a previously established adjacency. An asterisk (*) is prefixed to the neighbor entry for this state. 	All levels
Up Time	How long the adjacency has been up in one of the following formats: <ul style="list-style-type: none"> <i>nwndnh</i>—number of weeks, days, and hours <i>nd hh:mm:ss</i>—number of days, hours, minutes, and seconds 	brief detail none
Subscriber Count	Number of subscribers associated with the ANCP neighbor (access local loop).	brief none
Capabilities	Negotiated ANCP capability: <ul style="list-style-type: none"> Topo—Topology discovery. OAM—Performance of local Operations Administration Maintenance (OAM) procedures on an access loop controlled by the router. 	All levels
TCP Port	TCP port on which ANCP messages are exchanged.	detail
System Instance	Number identifying the ANCP link instance from the edge device's perspective.	detail
Peer Instance	Number identifying the ANCP instance from the access node's perspective. This number is unique and changes when the node or link comes back up after going down.	detail
Timer	Adjacency timer value advertised by the ANCP peer in 100 ms increments; the interval between ANCP ACK messages. This value remains constant for the duration of an ANCP session.	detail
Partition Type	Number that identifies whether partitions are used and how the ID is negotiated: <ul style="list-style-type: none"> 0—No partition. 1—Fixed partition requested. 2—Fixed partition assigned. 	detail
Partition Flag	Number that specifies the type of partition requested: 1 (new adjacency) or 2 (recovered adjacency).	detail
Partition Identifier	Number that associates the ANCP message with a specific partition.	detail

Table 9: show ancpc neighbor Output Fields (*continued*)

Field Name	Field Description	Level of Output
Partition Adjacencies	Number of adjacencies that share the partition.	detail
Dead Timer	Remaining period that the edge device waits for adjacency packets from a neighbor before declaring the neighbor to be down. The maximum dead time value is three times the configured adjacency timer value. This field displays the current value based on the time that the last adjacency packet was received.	detail
Received Syn Count	Number of synchronization messages received from neighbors to maintain adjacencies.	detail
Received Synack Count	Number of synchronization acknowledgment messages received from neighbors in response to the node's synchronization messages.	detail
Received Rstack Count	Number of messages received from neighbors indicating that the link to the neighbor needs to be reset.	detail
Received Ack Count	Number of acknowledgment messages periodically received from neighbors after an adjacency has been established.	detail
Received Port Up Count	Number of status messages received from neighbors indicating that a port has transitioned to the up state.	detail
Received Port Down Count	Number of status messages received from neighbors indicating that a port has transitioned to the down state.	detail
Received Generic Resp Count	Number of generic response messages received from neighbors.	detail
Received Adjacency Update Count	Number of adjacency update messages received from neighbors.	detail
Received OAM Count	Number of OAM responses received from neighbors in reply to request commands.	detail
Received Other Count	Number of all other ANCP message packets received from neighbors that do not fit into one of the other categories.	detail
Sent Syn Count	Number of synchronization messages sent to neighbors to maintain adjacencies.	detail
Sent Synack Count	Number of synchronization acknowledgment messages sent to neighbors in response to the their synchronization messages.	detail
Sent Rstack Count	Number of messages sent to neighbors indicating that the link to the neighbor needs to be reset.	detail
Sent Ack Count	Number of acknowledgment messages periodically sent to neighbors after an adjacency has been established.	detail

Table 9: show ancp neighbor Output Fields (*continued*)

Field Name	Field Description	Level of Output
Sent Generic Resp Count	Number of generic response messages sent to neighbors.	detail
Sent OAM Count	Number of OAM request commands sent to neighbors.	detail
Max Discovery Limit Exceed Count	Number of times that the maximum number of discovery table entries accepted from the neighbor has been exceeded.	detail
Result Codes	<p>Number of generic response messages sent to neighbors that include each of the following result codes:</p> <ul style="list-style-type: none"> • Invalid Request Message Count—A properly formed request message violated the protocol because of timing (such as a race condition) or direction of transmission. • Specified Port(s) Down Count—One or more of the specified ports are down because of a state mismatch between the router and an ANCP control application. • Out of Resources Count—ANCP is out of resources, probably not related to the access lines. This result code is sent only by an access node. • Request Msg Not Implemented Count— • Malformed Msg Count—Message is malformed because it was corrupted in transit or there was an implementation error at either end of the connection. • TLV Missing Count—One or more mandatory TLVs was missing from a request. • Invalid TLV Contents Count—The contents of one or more TLVs in the request do not match its required specification. • Non-Existent Port(s) Count—One or more of the ports specified in a request do not exist, possibly because of a configuration mismatch between the access node and the router or AAA. 	detail

Sample Output

show ancp neighbor

```

user@host> show ancp neighbor
  Version IP Address      PartID  State      Time      Subscriber
Capabilities
  0x31    10.0.1.3             0       Established 11:24      2          Topo
  0x31    10.0.1.5             0       Not Estblshd 2:45      2          Topo
* 0x0     100.0.0.2            0       Establishing 0          0
* 0x0     192.0.1.0            0       Configured   0          0
* 0x0     192.0.22.1           0       Configured   0          0

```

show ancp neighbor detail

```

user@host> show ancp neighbor detail
Neighbor Information
  Version      : 0x31
  IP Address    : 192.85.1.5
  System Name   : 00:10:94:00:00:01
  Up Time      : 26
  TCP Port     : 32666

```

```

State : Established
Subscriber Count : 4
Capabilities : Topo
System Instance : 2
Peer Instance : 20
Adjacency Timer (in 100ms) : 100
Peer Adjacency Timer (in 100ms) : 100
Partition Type : 0
Partition Flag : 1
Partition Identifier : 0
Partition Adjacencies : 0
Dead Timer : 23
Received Syn Count : 1
Received Synack Count : 1
Received Rstack Count : 0
Received Ack Count : 4
Received Port Up Count : 10
Received Port Down Count : 0
Received Generic Resp Count : 0
Received Adjacency Update Count : 0
Received OAM Count : 0
Received Other Count : 0
Sent Syn Count : 1
Sent Synack Count : 2
Sent Rstack Count : 0
Sent Ack Count : 3
Sent Generic Resp Count : 0
Sent OAM Count : 0
Max Discovery Limit Exceed Count : 0
Result Codes:
Invalid Request Message Count : 0 Received Sent
Specified Port(s) Down Count : 0 0
Out of Resources Count : 0 0
Request Msg Not Implemented Count: 0 0
Malformed Msg Count : 0 0
TLV Missing Count : 0 0
Invalid TLV Contents Count : 0 0
Non-Existent Port(s) Count : 0 0

Version : 0x32
IP Address : 192.168.9.1
System Name : 00:00:64:1c:01:02
Up Time : 36
TCP Port : 61408
State : Not Established
Subscriber Count : 1
Capabilities : Topology Discovery
System Instance : 12
Peer Instance : 1
Adjacency Timer (in 100ms) : 50
Peer Adjacency Timer (in 100ms) : 100
Partition Type : 0
Partition Flag : 1
Partition Identifier : 0
Partition Adjacencies : 0
Dead Timer : 23
Received Syn Count : 24
Received Synack Count : 20
Received Rstack Count : 2
Received Ack Count : 9

```

```

Received Port Up Count      : 5
Received Port Down Count    : 0
Received Generic Resp Count : 0
Received Adjacency Update Count : 0
Received OAM Responses Count : 2
Received Other Count        : 0
Sent Syn Count              : 20
Sent Synack Count           : 24
Sent Rstack Count           : 1
Sent Generic Resp Count     : 0
Sent Ack Count              : 9
Sent OAM Requests Count     : 4
Max Discovery Limit Exceed Count : 0
Result Codes:
Invalid Request Message Count : 0
Specified Port(s) Down Count  : 0
Out of Resources Count        : 0
Request Msg Not Implemented Count: 0
Malformed Msg Count          : 0
TLV Missing Count            : 0
Invalid TLV Contents Count    : 0
Non-Existent Port(s) Count    : 0

```

show ancp neighbor ip-address

```
user@host> show ancp neighbor ip-address 192.85.1.5
```

Neighbor Information

```

Version      : 0x32
IP Address   : 192.85.1.5
System Name  : ba:ad:be:ef:10:10
Up Time      : 26
TCP Port     : 32666
State        : Established
Subscriber Count : 4
Capabilities  : Topo
System Instance : 2
Peer Instance  : 20
Adjacency Timer (in 100ms) : 100
Peer Adjacency Timer (in 100ms) : 100
Partition Type : 0
Partition Flag : 1
Partition Identifier : 0
Partition Adjacencies : 0
Dead Timer    : 23
Received Syn Count : 1
Received Synack Count : 1
Received Rstack Count : 0
Received Ack Count : 4
Received Port Up Count : 10
Received Port Down Count : 0
Received Generic Resp Count : 0
Received Adjacency Update Count : 0
Received OAM Count : 0
Received Other Count : 0
Sent Syn Count : 1
Sent Synack Count : 2
Sent Rstack Count : 0
Sent Ack Count : 3
Sent Generic Resp Count : 0
Sent OAM Count : 0

```

Max Discovery Limit Exceed Count	: 0	
Result Codes:	Received	Sent
Invalid Request Message Count	: 0	0
Specified Port(s) Down Count	: 0	0
Out of Resources Count	: 0	0
Request Msg Not Implemented Count	: 0	0
Malformed Msg Count	: 0	0
TLV Missing Count	: 0	0
Invalid TLV Contents Count	: 0	0
Non-Existent Port(s) Count	: 0	0

show ancp neighbor system-name

user@host> show ancp neighbor ba:ad:be:ef:10:10 detail

Neighbor Information

Version	: 0x31	
IP Address	: 10.100.0.1	
System Name	: 00:00:64:1b:01:02	
Up Time	: 19	
TCP Port	: 1028	
State	: Established	
Subscriber Count	: 2	
Capabilities	: Topology Discovery, OAM	
System Instance	: 1	
Peer Instance	: 10	
Adjacency Timer (in 100ms)	: 100	
Peer Adjacency Timer (in 100ms)	: 250	
Partition Type	: 0	
Partition Flag	: 1	
Partition Identifier	: 0	
Partition Adjacencies	: 0	
Dead Timer	: 55	
Received Syn Count	: 1	
Received Synack Count	: 1	
Received Rstack Count	: 0	
Received Ack Count	: 1	
Received Port Up Count	: 34	
Received Port Down Count	: 0	
Received Generic Resp Count	: 0	
Received Adjacency Update Count	: 0	
Received OAM Responses Count	: 2	
Received Other Count	: 0	
Sent Syn Count	: 1	
Sent Synack Count	: 1	
Sent Rstack Count	: 0	
Sent Ack Count	: 3	
Sent Generic Resp Count	: 0	
Sent OAM Requests Count	: 4	
Max Discovery Limit Exceed Count	: 3	
Result Codes:	Received	Sent
Invalid Request Message Count	: 0	0
Specified Port(s) Down Count	: 0	0
Out of Resources Count	: 0	0
Request Msg Not Implemented Count	: 0	0
Malformed Msg Count	: 0	0
TLV Missing Count	: 0	0
Invalid TLV Contents Count	: 0	0
Non-Existent Port(s) Count	: 0	0

show ancp statistics

Syntax	show ancp statistics <ip-address <i>ip-address</i> > <system-name <i>mac-address</i> >
Release Information	Command introduced in Junos OS Release 13.3.
Description	Display statistics for all ANCP neighbors (access nodes) or the specified ANCP neighbor.
Options	<p>none—Display statistics for all ANCP neighbors, including global statistics not show for individual neighbors.</p> <p>ip-address <i>ip-address</i>—(Optional) Display statistics for only the neighbor with the specified IP address.</p> <p>system-name <i>mac-address</i>—(Optional) Display statistics for only the neighbor with the specified MAC address.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp cos on page 108 • show ancp neighbor on page 111 • show ancp subscriber on page 124
List of Sample Output	show ancp statistics on page 121 show ancp statistics ip-address on page 122 show ancp statistics system-name on page 122
Output Fields	Table 10 on page 119 lists the output fields for the show ancp statistics command. Output fields are listed in the approximate order in which they appear.

Table 10: show ancp statistics Output Fields

Field Name	Field Description
Number of neighbors	Total count of ANCP neighbors.
Number of subscribers	Total count of ANCP subscribers.
Accept Count	Number of neighbor TCP/IP sessions accepted on listener socket.
Accept Fail Count	Number of neighbor TCP/IP sessions that failed due to one of the following causes: session already exists, maximum number of ANCP connections exceeded, creation of session or neighbor failed, or protocol start failed.

Table 10: show ancp statistics Output Fields (*continued*)

Field Name	Field Description
No Config Accept Deny Count	Number of neighbor TCP/IP sessions that failed because the neighbor was not configured.
Received Syn Count	Number of synchronization messages received from neighbors to maintain adjacencies.
Received Synack Count	Number of synchronization acknowledgment messages received from neighbors in response to the node's synchronization messages.
Received Rstack Count	Number of messages received from neighbors indicating that the link to the neighbor needs to be reset.
Received Ack Count	Number of acknowledgment messages periodically received from neighbors after an adjacency has been established.
Received Port Up Count	Number of status messages received from neighbors indicating that a port has transitioned to the up state.
Received Port Down Count	Number of status messages received from neighbors indicating that a port has transitioned to the down state.
Received Generic Resp Count	Number of generic response messages received from neighbors.
Received Adjacency Update Count	Number of adjacency update messages received from neighbors.
Received OAM Count	Number of OAM responses received from neighbors in reply to request commands.
Received Other Count	Number of all other ANCP message packets received from neighbors that do not fit into one of the other categories.
Sent Syn Count	Number of synchronization messages sent to neighbors to maintain adjacencies.
Sent Synack Count	Number of synchronization acknowledgment messages sent to neighbors in response to the their synchronization messages.
Sent Rstack Count	Number of messages sent to neighbors indicating that the link to the neighbor needs to be reset.
Sent Ack Count	Number of acknowledgment messages periodically sent to neighbors after an adjacency has been established.
Sent Generic Resp Count	Number of generic response messages sent to neighbors.
Sent OAM Count	Number of OAM request commands sent to neighbors.

Table 10: show ancp statistics Output Fields (*continued*)

Field Name	Field Description
Result Codes	<p>Number of generic response messages sent to neighbors that include each of the following result codes:</p> <ul style="list-style-type: none"> • Invalid Request Message Count—A properly formed request messages violated the protocol because of timing (such as a race condition) or direction of transmission. • Specified Port(s) Down Count—One or more of the specified ports are down because of a state mismatch between the router and an ANCP control application. • Out of Resources Count—the ANCP agent is out of resources, probably not related to the access lines. This result code is sent only by an access node. • Request Msg Not Implemented Count— • Malformed Msg Count—Message is malformed because it was corrupted in transit or there was an implementation error at either end of the connection. • TLV Missing Count—One or more mandatory TLVs was missing from a request. • Invalid TLV Contents Count—The contents of one or more TLVs in the request do not match its required specification. • Non-Existent Port(s) Count—One or more of the ports specified in a request do not exist, possibly because of a configuration mismatch between the access node and the router or AAA.

Sample Output

show ancp statistics

```

user@host> show ancp statistics
Statistics
  Number of neighbors           : 4
  Number of subscribers        : 6
  Accept Count                  : 0
  Accept Fail Count             : 0
  No Config Accept Deny Count  : 0
  Received Syn Count            : 2
  Received Synack Count         : 1
  Received Rstack Count         : 0
  Received Ack Count            : 8
  Received Port Up Count        : 7
  Received Port Down Count      : 0
  Received Generic Resp Count   : 0
  Received Adjacency Update Count : 0
  Received OAM Count            : 0
  Received Other Count          : 0
  Sent Syn Count                : 1
  Sent Synack Count             : 1
  Sent Rstack Count             : 0
  Sent Ack Count                : 17
  Sent Generic Resp Count       : 0
  Sent OAM Count                : 4
Result Codes:
  Invalid Request Message Count : 0
  Specified Port(s) Down Count  : 0
  Out of Resources Count        : 0
  Request Msg Not Implemented Count: 0
Received Sent

```

Malformed Msg Count	: 0	0
TLV Missing Count	: 0	0
Invalid TLV Contents Count	: 0	0
Non-Existent Port(s) Count	: 0	0

show ancp statistics ip-address

```
user@host> show ancp statistics ip-address 10.0.0.1
Statistics
  Received Syn Count           : 2
  Received Synack Count       : 1
  Received Rstack Count       : 0
  Received Ack Count          : 8
  Received Port Up Count      : 7
  Received Port Down Count    : 0
  Received Generic Resp Count : 0
  Received Adjacency Update Count : 0
  Received OAM Count          : 0
  Received Other Count        : 0
  Sent Syn Count              : 1
  Sent Synack Count           : 1
  Sent Rstack Count           : 0
  Sent Ack Count              : 17
  Sent Generic Resp Count     : 0
  Sent OAM Count              : 4
Result Codes:
  Received Sent
  Invalid Request Message Count : 0 0
  Specified Port(s) Down Count : 0 0
  Out of Resources Count        : 0 0
  Request Msg Not Implemented Count: 0 0
  Malformed Msg Count          : 0 0
  TLV Missing Count            : 0 0
  Invalid TLV Contents Count    : 0 0
  Non-Existent Port(s) Count   : 0 0
```

show ancp statistics system-name

```
user@host> show ancp statistics system-name 00:00:64:1b:01:02
Statistics
  Received Syn Count           : 2
  Received Synack Count       : 1
  Received Rstack Count       : 0
  Received Ack Count          : 8
  Received Port Up Count      : 7
  Received Port Down Count    : 0
  Received Generic Resp Count : 0
  Received Adjacency Update Count : 0
  Received OAM Count          : 0
  Received Other Count        : 0
  Sent Syn Count              : 1
  Sent Synack Count           : 1
  Sent Rstack Count           : 0
  Sent Ack Count              : 17
  Sent Generic Resp Count     : 0
  Sent OAM Count              : 4
Result Codes:
  Received Sent
  Invalid Request Message Count : 0 0
  Specified Port(s) Down Count : 0 0
  Out of Resources Count        : 0 0
```

Request Msg Not Implemented Count:	0	0
Malformed Msg Count	: 0	0
TLV Missing Count	: 0	0
Invalid TLV Contents Count	: 0	0
Non-Existent Port(s) Count	: 0	0

show ancp subscriber

Syntax	show ancp subscriber <brief detail> <identifier <i>identifier</i>> <neighbor <i>ip-address</i>>
Release Information	Command introduced in Junos OS Release 9.4.
Description	Display information about active subscribers regardless of the subscriber's operational state, for all subscribers (local access loops), the subscriber associated with the access line specified by an ACL, or the subscriber associated with the specified ANCP neighbor (access node).
Options	<p>brief detail—(Optional) Display the specified level of detail.</p> <p>identifier <i>identifier</i>—(Optional) Display information about the subscriber associated with the access line specified by the access identifier.</p> <p>neighbor <i>ip-address</i>—(Optional) Display information about the subscribers connected to the access node specified by the IP address.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear ancp subscriber on page 104 • show ancp cos on page 108 • show ancp neighbor on page 111
List of Sample Output	show ancp subscriber on page 127 show ancp subscriber brief on page 127 show ancp subscriber detail on page 127 show ancp subscriber identifier identifier-string detail on page 128
Output Fields	Table 11 on page 124 lists the output fields for the show ancp subscriber command. Output fields are listed in the approximate order in which they appear.

Table 11: show ancp subscriber Output Fields

Field Name	Field Description	Level of Output
Loop Identifier	<p>Access loop identifier as sent by the access node and configured to map the subscriber to an interface.</p> <p>An asterisk (*) indicates that the information might be stale due to receiving a Port Down message with a DSL Line State of Idle.</p> <p>Two asterisks (**) indicate that the neighbor associated with the subscriber has lost its adjacency. In this case, the DSL Line State might be Established.</p>	brief none
DSL Line State	State of the DSL line: Idle , Showtime , or Silent .	brief detail

Table 11: show ancp subscriber Output Fields (*continued*)

Field Name	Field Description	Level of Output
Type	Type of digital subscriber line employed by the access node: ADSL1 , ADSL2 , ADSL2+ , VDSL1 , VDSL2 , SDSL , or UNKNOWN .	brief none
Interface	Name of the interface set or logical interface.	brief detail none
Rate Kbps	Actual downstream data rate for this local loop.	brief none
Neighbor	IP address of ANCP neighbor (access node).	brief none
Access Loop Circuit Identifier	<p>Access loop circuit identifier as sent by the access node and configured to map the subscriber to an interface.</p> <p>An asterisk (*) indicates that the information might be stale due to receiving a Port Down message with a DSL Line State of Idle.</p> <p>Two asterisks (**) indicate that the neighbor associated with the subscriber has lost its adjacency. In this case, the DSL Line State might be Established.</p>	detail
Neighbor IP Address	IP address of the ANCP neighbor (access node).	detail
Aggregate Circuit Identifier Binary	Binary identifier for the VLAN circuit ID.	detail
DSL Type	Type of digital subscriber line employed by the access node: ADSL1 , ADSL2 , ADSL2+ , VDSL1 , VDSL2 , SDSL , or UNKNOWN .	detail
DSL Line Data Link	Data link protocol employed on the access loop: AAL5 or Ethernet .	detail
DSL Line Encapsulation	<p>Encapsulation type on the access loop, for Ethernet only:</p> <ul style="list-style-type: none"> 0—NA, type not conveyed 1—Untagged Ethernet 2—Single-tagged Ethernet 	detail
DSL Line Encapsulation Payload	<p>Payload carried across the access loop:</p> <ul style="list-style-type: none"> 0—NA, type not conveyed 1—PPPoA LLC 2—PPPoA null 3—IPoA LLC 4—IPoA null 5—Ethernet over AAL5 LLC with FCS 6—Ethernet over AAL5 LLC without FCS 7—Ethernet over AAL5 null with FCS 8—Ethernet over AAL5 null without FCS 	detail
Interface Type	Type of interface employed for subscriber traffic: ifl for a single VLAN or interface-set for a configured group of VLANs.	detail

Table 11: show ancp subscriber Output Fields (*continued*)

Field Name	Field Description	Level of Output
Actual Net Data Upstream	Actual upstream data rate for this local loop, in Kbps.	detail
Actual Net Data Downstream	Actual downstream data rate for this local loop, in Kbps.	detail
Minimum Net Data Upstream	Minimum upstream data rate desired by the operator for this local loop, in Kbps.	detail
Minimum Net Data Downstream	Minimum downstream data rate desired by the operator for this local loop, in Kbps.	detail
Maximum Net Data Upstream	Maximum upstream data rate desired by the operator for this local loop, in Kbps.	detail
Maximum Net Data Downstream	Maximum downstream data rate desired by the operator for this local loop, in Kbps.	detail
Attainable Net Data Upstream	Maximum attainable upstream data rate for this local loop, in Kbps.	detail
Attainable Net Data Downstream	Maximum attainable downstream data rate for this local loop, in Kbps.	detail
Minimum Low Power Data Downstream	Minimum downstream data rate desired by the operator for this local loop in low power state, in Kbps.	detail
Minimum Low Power Data Upstream	Minimum upstream data rate desired by the operator for this local loop in low power state, in Kbps.	detail
Maximum Interleave Delay Downstream	Maximum interleaving delay for downstream data, in milliseconds.	detail
Maximum Interleave Delay Upstream	Maximum interleaving delay for upstream data, in milliseconds.	detail
Actual Interleave Delay Downstream	Actual interleaving delay for downstream data, in milliseconds.	detail
Actual Interleave Delay Upstream	Actual interleaving delay for upstream data, in milliseconds.	detail

Sample Output

show ancp subscriber

```
user@host> show ancp subscriber
```

Loop Identifier	DSL Line State	Type	Interface	Rate Kbps	Neighbor
**circuit 101	Idle	ADSL1	----	32	10.0.1.3
**circuit 102	Idle	ADSL1	----	32	10.0.1.3
circuit 301	Showtime	ADSL1	----	32	10.0.1.5
circuit 302	Showtime	ADSL1	----	32	10.0.1.5

show ancp subscriber brief

```
user@host> show ancp subscriber brief
```

Loop Identifier	Type	Interface	Rate Kbps	Neighbor
port-1-10	VDSL2	set-ge-10410	64	10.10.10.2
port-1-11	VDSL2	set-ge-10411	64	11.11.11.2
port-2-10	VDSL2	ge-1/0/4.12	64	10.12.12.2
port-2-11	VDSL2	ge-1/0/4.13	64	10.13.13.2

show ancp subscriber detail

```
user@host> show ancp subscriber detail
```

Subscriber Information

- * Access Loop Circuit Identifier : circuit 101
 - Neighbor IP Address : 10.0.1.3
 - Aggregate Circuit Identifier Binary : 0/0
 - DSL Type : ADSL1
 - DSL Line State : Idle
 - DSL Line Data Link : Data link 2
 - DSL Line Encapsulation : N/A
 - DSL Line Encapsulation Payload : N/A
 - Interface Type : N/A
 - Interface : ----
 - Actual Net Data Upstream : 32
 - Actual Net Data Downstream : 32
 - Minimum Net Data Upstream : 0
 - Minimum Net Data Downstream : 0
 - Maximum Net Data Upstream : 0
 - Maximum Net Data Downstream : 0
 - Attainable Net Data Upstream : 1024
 - Attainable Net Data Downstream : 8192
 - Minimum Low Power Data Downstream : 32
 - Minimum Low Power Data Upstream : 32
 - Maximum Interleave Delay Downstream : 20
 - Maximum Interleave Delay Upstream : 20
 - Actual Interleave Delay Downstream : 20
 - Actual Interleave Delay Upstream : 20
- * Access Loop Circuit Identifier: circuit 102
 - Neighbor IP Address : 10.0.1.3
 - Aggregate Circuit Identifier Binary : 0/0
 - DSL Type : ADSL1
 - DSL Line State : Idle
 - DSL Line Data Link : Data link 2
 - DSL Line Encapsulation : N/A
 - DSL Line Encapsulation Payload : N/A

```
Interface Type           : N/A
Interface                 : ----
Actual Net Data Upstream  : 32
Actual Net Data Downstream : 32
Minimum Net Data Upstream : 0
Minimum Net Data Downstream : 0
Maximum Net Data Upstream : 0
Maximum Net Data Downstream : 0
Attainable Net Data Upstream : 1024
Attainable Net Data Downstream : 8192
Minimum Low Power Data Downstream : 32
Minimum Low Power Data Upstream : 32
Maximum Interleave Delay Downstream : 20
Maximum Interleave Delay Upstream : 20
Actual Interleave Delay Downstream : 20
Actual Interleave Delay Upstream : 20
...
```

show ancp subscriber identifier identifier-string detail

```
user@host> show ancp subscriber identifier port-1-11 detail
```

```
Access Loop Identifier : port-1-11
Neighbor IP Address    : 10.11.11.2
Aggregate Circuit Identifier Binary : 0/0
DSL Type               : DSL 0
Interface Type         : interface-set
Interface              : set-ge-10411
DSL Line State         : Show Time
Actual Net Data Upstream : 64
Actual Net Data Downstream : 64
DSL Line Data Link     : AAL5
DSL Line Encapsulation : N/A
DSL Line Encapsulation Payload : N/A
Minimum Net Data Upstream : 64
Minimum Net Data Downstream : 64
Maximum Net Data Upstream : 64
Maximum Net Data Downstream : 64
Attainable Net Data Upstream : 64
Attainable Net Data Downstream : 64
Minimum Low Power Data Downstream : 64
Minimum Low Power Data Upstream : 64
Maximum Interleave Delay Downstream : 50
Maximum Interleave Delay Upstream : 50
Actual Interleave Delay Downstream : 50
Actual Interleave Delay Upstream : 50
```


show ancp summary

Syntax	show ancp summary
Release Information	Command introduced in Junos OS Release 13.1.
Description	Display a summary of the counts and states for all ANCP neighbors and subscribers.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp neighbor on page 111 • show ancp summary neighbor on page 131 • show ancp subscriber on page 124 • show ancp summary subscriber on page 133
List of Sample Output	show ancp summary on page 130
Output Fields	Table 12 on page 129 lists the output fields for the show ancp summary command. Output fields are listed in the approximate order in which they appear.

Table 12: show ancp summary Output Fields

Field Name	Field Description
Configured	Number of ANCP neighbors in the Configured state; that is, that have been configured but never established.
Establishing	Number of ANCP neighbors in the Establishing state; that is, where negotiations are in progress.
Established	Number of ANCP neighbors in the Established state; that is, where negotiations have succeeded and the ANCP session has been established.
Not Estblshd	Number of ANCP neighbors in the Not Estblshd state; that is, that have lost a previously established adjacency and are ready to begin negotiations.
Total	Total number of ANCP neighbors; sum of neighbors in the Configured , Establishing , Established , and Not Estblshd states.
Showtime	Number of DSL lines in Showtime state.
Idle	Number of DSL lines in Idle state.
Silent	Number of DSL lines in Silent state.
Unknown	Number of DSL lines where the state is not Showtime , Idle , or Silent .

Table 12: show ancp summary Output Fields (*continued*)

Field Name	Field Description
Total	Total number of DSL lines (ANCP subscribers); sum of DSL lines in the Showtime , Idle , Silent , and Unknown states.

Sample Output

show ancp summary

```
user@host> show ancp summary
```

Neighbors Summary:

Configured	Establishing	Established	Not Established	Total
22	0	2	0	24

Subscribers Summary:

Showtime	Idle	Silent	Unknown	Total
4	0	0	0	4

show ancp summary neighbor

Syntax	show ancp summary neighbor <ip-address <i>ip-address</i> system-name <i>mac-address</i> >
Release Information	Command introduced in Junos OS Release 13.1.
Description	Display a summary of the counts and states for all ANCP neighbors and of the neighbor's subscribers when you specify a particular neighbor.
Options	ip-address <i>ip-address</i> —(Optional) IP address of the ANCP neighbor (access node). system-name <i>mac-address</i> —(Optional) MAC address of the ANCP neighbor (access node).
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp summary on page 129 • show ancp subscriber on page 124 • show ancp summary subscriber on page 133
List of Sample Output	show ancp summary neighbor on page 132 show ancp summary neighbor (IP Address) on page 132 show ancp summary neighbor (MAC Address) on page 132
Output Fields	Table 13 on page 131 lists the output fields for the show ancp summary command. Output fields are listed in the approximate order in which they appear.

Table 13: show ancp summary neighbor Output Fields

Field Name	Field Description
Configured	Number of ANCP neighbors in the Configured state; that is, that have been configured but never established.
Establishing	Number of ANCP neighbors in the Establishing state; that is, where negotiations are in progress.
Established	Number of ANCP neighbors in the Established state; that is, where negotiations have succeeded and the ANCP session has been established.
Not Estblshd	Number of ANCP neighbors in the Not Estblshd state; that is, that have lost a previously established adjacency and are ready to begin negotiations.
Total	Total number of ANCP neighbors; sum of neighbors in the Configured , Establishing , Established , and Not Estblshd states.
Showtime	Number of DSL lines for the neighbor in Showtime state.

Table 13: show ancp summary neighbor Output Fields (*continued*)

Field Name	Field Description
Idle	Number of DSL lines for the neighbor in Idle state.
Silent	Number of DSL lines for the neighbor in Silent state.
Unknown	Number of DSL lines for the neighbor where the state is not Showtime , Idle , or Silent .
Total	Total number of DSL lines (ANCP subscribers); sum of DSL lines in the Showtime , Idle , Silent , and Unknown states.

Sample Output

show ancp summary neighbor

```
user@host> show ancp summary neighbor
```

Neighbors Summary:

Configured	Establishing	Established	Not Established	Total
22	0	2	0	24

show ancp summary neighbor (IP Address)

```
user@host> show ancp summary neighbor ip-address 192.168.10.1
```

Neighbor Summary:192.168.10.1 status Established

Subscribers Summary:

Show Time	Idle	Silent	Unknown	Total
6	0	0	0	6

show ancp summary neighbor (MAC Address)

```
user@host> show ancp summary neighbor system-name 00:00:64:1b:01:02
```

Neighbor Summary:00:00:64:1b:01:02 status Established

Subscribers Summary:

Show Time	Idle	Silent	Unknown	Total
5	1	2	0	8

show ancp summary subscriber

Syntax	show ancp summary subscriber
Release Information	Command introduced in Junos OS Release 13.1.
Description	Display a summary of the counts and states for all ANCP subscribers.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp summary on page 129 • show ancp neighbor on page 111 • show ancp summary neighbor on page 131
List of Sample Output	show ancp summary subscriber on page 133
Output Fields	Table 14 on page 133 lists the output fields for the show ancp summary subscriber command. Output fields are listed in the approximate order in which they appear.

Table 14: show ancp summary subscriber Output Fields

Field Name	Field Description
Showtime	Number of DSL lines in Showtime state.
Idle	Number of DSL lines in Idle state.
Silent	Number of DSL lines in Silent state.
Unknown	Number of DSL lines where the state is not Showtime , Idle , or Silent .
Total	Total number of DSL lines (ANCP subscribers); sum of DSL lines in the Showtime , Idle , Silent , and Unknown states.

Sample Output

show ancp summary subscriber

```
user@host> show ancp summary subscriber
```

```
Subscribers Summary:
Show Time   Idle      Silent     Unknown    Total
-----
           8         1         0          1        10
```


PART 4

Troubleshooting

- [Acquiring Troubleshooting Information on page 137](#)
- [Troubleshooting Configuration Statement on page 143](#)

CHAPTER 8

Acquiring Troubleshooting Information

- [Tracing ANCP Agent Operations for Subscriber Access on page 137](#)
- [Configuring the ANCP Trace Log Filename on page 138](#)
- [Configuring the Number and Size of ANCP Log Files on page 138](#)
- [Configuring Access to the ANCP Log File on page 139](#)
- [Configuring a Regular Expression for ANCP Messages to Be Logged on page 139](#)
- [Configuring the ANCP Tracing Flags on page 140](#)
- [Configuring the Severity Level to Filter Which ANCP Messages Are Logged on page 140](#)
- [Collecting Subscriber Access Logs Before Contacting Juniper Technical Support on page 141](#)

Tracing ANCP Agent Operations for Subscriber Access

The Junos OS trace feature tracks ANCP agent operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename **ancpd**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file **filename** reaches 128 kilobytes (KB), it is compressed and renamed **filename.0.gz**. Subsequent events are logged in a new file called **filename**, until it reaches capacity again. At this point, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure ANCP agent tracing operations:

1. (Optional) Configure a trace log filename.
See [“Configuring the ANCP Trace Log Filename” on page 138](#).
2. (Optional) Configure the number and size of trace logs.
See [“Configuring the Number and Size of ANCP Log Files” on page 138](#).
3. (Optional) Configure user access to trace logs.
See [“Configuring Access to the ANCP Log File” on page 139](#).
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.
See [“Configuring a Regular Expression for ANCP Messages to Be Logged” on page 139](#).
5. (Optional) Configure flags to specify which events are logged.
See [“Configuring the ANCP Tracing Flags” on page 140](#).
6. (Optional) Configure a severity level for messages to specify which event messages are logged.
See [“Configuring the Severity Level to Filter Which ANCP Messages Are Logged” on page 140](#).

Related Documentation • [Configuring the ANCP Agent on page 29](#)

Configuring the ANCP Trace Log Filename

By default, the name of the file that records trace output for ANCP is **ancpd**. You can specify a different name with the **file** option.

To configure the filename for ANCP tracing operations:

- Specify the name of the file used for the trace output.

```
[edit protocols ancp traceoptions]  
user@host# set file ancp_1
```

Related Documentation • [Tracing ANCP Agent Operations for Subscriber Access on page 137](#)

Configuring the Number and Size of ANCP Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format *.number.gz*. The newest archived file is *.0.gz* and the oldest archived file is *.(maximum number)-1.gz*. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, *filename*, reaches 2 MB, *filename* is compressed and renamed *filename.0.gz*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until there are 20 trace files. Then the oldest file, *filename.19.gz*, is simply overwritten when the next oldest file, *filename.18.gz* is compressed and renamed to *filename.19.gz*.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1_logfile_1 files 20 size 2097152
```

Related Documentation

- [Tracing ANCP Agent Operations for Subscriber Access on page 137](#)

Configuring Access to the ANCP Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1_logfile_1 world-readable
```

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1_logfile_1 no-world-readable
```

Related Documentation

- [Tracing ANCP Agent Operations for Subscriber Access on page 137](#)

Configuring a Regular Expression for ANCP Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events.

You can refine the output by including regular expressions to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit protocols ancp traceoptions]  
user@host# set file ancp_1_logfile_1 match regex
```

**Related
Documentation**

- [Tracing ANCP Agent Operations for Subscriber Access on page 137](#)

Configuring the ANCP Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit protocols ancp traceoptions]  
user@host# set flag restart
```

**Related
Documentation**

- [Tracing ANCP Agent Operations for Subscriber Access on page 137](#)

Configuring the Severity Level to Filter Which ANCP Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages. By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

```
[edit protocols ancp traceoptions]  
user@host# set level severity
```

**Related
Documentation**

- [Tracing ANCP Agent Operations for Subscriber Access on page 137](#)
- [Configuring the ANCP Agent on page 29](#)
- [traceoptions on page 89](#)

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

```
user@host> request support information | save rsi-1
```

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

```
[edit]
set system syslog archive size 100m files 25
set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all
set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all
set interfaces pp0 traceoptions flag all
set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all
set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all
set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25
set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

2. Copy the relevant statements into a text file and modify the log filenames as you want.

3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.



.....

NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

.....



.....

BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

.....

**Related
Documentation**

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*

CHAPTER 9

Troubleshooting Configuration Statement

- [traceoptions \(ANCP\) on page 144](#)

traceoptions (ANCP)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i> <disable>; level (all error info notice verbose warning); no-remote-trace; }</pre>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Define tracing operations for ANCP agent processes.
Options	<p>file <i>filename</i>— Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>— (Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. Include the disable option after a flag to disable tracing for that flag. You can include the following flags:</p> <ul style="list-style-type: none">• all—Trace all operations.• config—Trace configuration events.• cos—Trace class-of-service events.• general—Trace general flow.• packet—Trace ANCP packet transmit and receive operations.• process—Trace process internals.• protocol—Trace protocol events.• restart—Trace process restart flow• routing-socket—Trace routing socket events.• session—Trace connection events and flow.• startup—Trace ANCP startup events and flow.• subscriber—Trace subscriber events.• timer—Trace timer processing. <p>level—Level of tracing to perform. You can specify any of the following levels:</p>

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none"> • Tracing ANCP Agent Operations for Subscriber Access on page 137
------------------------------	---

PART 5

Index

- [Index on page 149](#)

Index

Symbols

#, comments in configuration statements.....	xiv
(), in syntax descriptions.....	xiv
< >, in syntax descriptions.....	xiv
[], in configuration statements.....	xiv
{ }, in configuration statements.....	xiv
(pipe), in syntax descriptions.....	xiv

A

AAA	
ANCP interactions.....	13
access loop circuit identifier	
ANCP.....	5
configuring ANCP.....	32
access profile statements	
ancp-speed-change-immediate-update.....	71
access-identifier statement	
ANCP.....	67
ACI	
ANCP.....	5
adjacency timer	
ANCP global configuration.....	33
ANCP neighbor configuration.....	31, 33
adjacency-timer statement	
ANCP.....	68
advisory-options statement	
ANCP.....	69
L2TP.....	69
ANCP	
AAA interactions.....	13
access loop circuit identifier.....	5
access loop circuit identifier configuration.....	32
ACI.....	5
adjacency timer global configuration.....	33
adjacency timer neighbor configuration.....	33
adjusting subscriber line traffic	
rates.....	36, 38, 40
adjusting subscriber traffic with.....	10
associating subscriber VLANs with access	
nodes.....	32

backwards compatibility global	
configuration.....	34
backwards compatibility neighbor	
configuration.....	31, 34
clearing statistics.....	102
configuration overview.....	29
CoS information	
verifying.....	97
CoS shaping across restarts.....	25
CoS shaping rate adjustment for subscriber	
local loops.....	10
CoS state	
displaying ANCP.....	108
discovery table global configuration.....	34
discovery table neighbor configuration.....	31, 34
event logging.....	137
flags for tracing operations.....	140
immediate interim-accounting messages.....	41
local access loop	
displaying.....	124
log file access for tracing operations.....	139
log file size and number.....	138
log filenames for tracing operations.....	138
message severity levels for tracing	
operations.....	140
monitoring subscriber traffic with.....	3
neighbor	
clearing.....	100
neighbor configuration	
adjacency timer.....	31
discovery table entries.....	31
ietf mode.....	31
IP address.....	31
pre-ietf mode.....	31
neighbor information	
clearing.....	96
verifying.....	95
neighbor summary	
displaying.....	131
neighbors	
displaying.....	111
operations in different access models.....	15
overview.....	3
partition ID learning.....	35
pre-ietf mode global configuration.....	34
pre-ietf mode neighbor configuration.....	31, 34
regular expressions for tracing operations.....	139
reporting traffic to CoS.....	37
request OAM per interface.....	106

request OAM per neighbor.....	107	traceoptions.....	89, 144
restart time global configuration.....	35	underlying-interface.....	91
statistics		upstream-rate.....	92
displaying.....	119	ancp-speed-change-immediate-update statement	
statistics information		ANCP.....	71
clearing.....	97	B	
subscriber		backwards compatibility	
clearing.....	104	ANCP global configuration.....	34
subscriber information		ANCP neighbor configuration.....	31, 34
clearing.....	97	braces, in configuration statements.....	xiv
verifying.....	96	brackets	
subscriber summary		angle, in syntax descriptions.....	xiv
displaying.....	133	square, in configuration statements.....	xiv
subscribers		C	
displaying.....	124	clear ancp neighbor command.....	100
summary		clear ancp statistics command.....	102
displaying.....	129	clear ancp subscriber command.....	104
tracing operations.....	137	comments, in configuration statements.....	xiv
triggering OAM		conventions	
local loop.....	41	text and syntax.....	xiii
ANCP agent <i>See</i> ANCP		CoS	
ancp statement		shaping preserved across ANCP restarts.....	25
ANCP.....	70	CoS traffic shaping	
ANCP statements		with ANCP.....	38, 40
access-identifier.....	67	curly braces, in configuration statements.....	xiv
adjacency-timer.....	68	customer support.....	xv
advisory-options.....	69	contacting JTAC.....	xv
ancp.....	70	D	
ancp-speed-change-immediate-update.....	71	discovery table	
downstream-rate.....	72	ANCP global configuration.....	34
gsmp-syn-timeout.....	77	ANCP neighbor configuration.....	31, 34
gsmp-syn-wait.....	78	documentation	
ietf-mode.....	78	comments on.....	xv
interface-set.....	79	downstream-rate statement	
interfaces.....	80	ANCP.....	72
juniper-dsl-attributes.....	81	L2TP.....	72
maximum-discovery-table-entries.....	82	DSL Forum VSAs	
maximum-helper-restart-time.....	82	ANCP.....	23
neighbor		E	
for all neighbors.....	83	exclude statement.....	73
overhead-accounting.....	84	F	
pre-ietf-mode.....	85	font conventions.....	xiii
qos-adjust.....	85		
qos-adjust-adsl.....	86		
qos-adjust-adsl2.....	86		
qos-adjust-adsl2-plus.....	87		
qos-adjust-sdsl.....	87		
qos-adjust-vdsl.....	88		
qos-adjust-vdsl2.....	88		

G

gsmp-syn-timeout statement	
ANCP	77
gsmp-syn-wait statement	
ANCP	78

I

ietf-mode statement	
ANCP	78
interface-set statement	
ANCP	79
interfaces statement	
ANCP	80
interim accounting	
ANCP immediate updates	41

J

juniper-dsl-attributes statement	
RADIUS	81

L

L2TP statements	
LAC	
advisory-options	69
downstream-rate	72
upstream-rate	92
log files	
collecting for Juniper Technical Support	141
configuring ANCP trace	137
number of ANCP	138
size of ANCP	138

M

manuals	
comments on	xv
maximum-discovery-table-entries statement	
ANCP	82
maximum-helper-restart-time statement	
ANCP	82

N

neighbor	
ANCP	100
parameters for ANCP	31
neighbor statement	
ANCP	
for all neighbors	83

O

OAM	
triggering ANCP	41
overhead-accounting statement	
ANCP	84

P

parentheses, in syntax descriptions	xiv
partition ID	
learning ANCP	35
pre-ietf mode	
ANCP global configuration	34
ANCP neighbor configuration	31, 34
pre-ietf-mode statement	
ANCP	85

Q

qos-adjust statement	
ANCP	85
qos-adjust-adsl statement	
ANCP	86
qos-adjust-adsl2 statement	
ANCP	86
qos-adjust-adsl2-plus statement	
ANCP	87
qos-adjust-sdsl statement	
ANCP	87
qos-adjust-vdsl statement	
ANCP	88
qos-adjust-vdsl2 statement	
ANCP	88

R

RADIUS statements	
juniper-dsl-attributes	81
request ancp oam interface command	106
request ancp oam neighbor command	107
restart time	
ANCP global configuration	35

S

shaping-rate adjustments	
for subscriber local loops	10
show ancp cos command	108
show ancp neighbor command	111
show ancp statistics command	119
show ancp subscriber command	124
show ancp summary command	129
show ancp summary neighbor command	131

show ancp summary subscriber command.....	133
subscriber	
ANCP.....	104
subscriber local loops	
CoS shaping-rate adjustments with ANCP.....	10
subscribers	
identifying ANCP.....	32
support, technical See technical support	
syntax conventions.....	xiii

T

technical support	
collecting logs for.....	141
contacting JTAC.....	xv
trace operations	
collecting logs for Juniper technical support.....	141
tracoptions statement	
ANCP.....	89, 144
tracing operations	
ANCP.....	137
traffic shaping	
adjustment of ANCP.....	36, 38, 40
ANCP-agent reported rates for CoS.....	37
troubleshooting subscriber access	
collecting logs for Juniper Technical Support.....	141

U

underlying-interface statement	
ANCP interface set.....	91
upstream-rate statement	
ANCP.....	92
L2TP.....	92

V

VSAs	
ANCP-related DSL Forum.....	23