JUNIPER NETWORKS

Junos® OS

PPP Feature Guide for Subscriber Management

Release
14.1.1

Published: 2014-05-08

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

Junos® OS PPP Feature Guide for Subscriber Management
141.1

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

List of Figures

List of Tables

About the Documentation

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.xsl;
       }
     }
   }
   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.xsl; }
   ```

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.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• 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*** **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (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.	• 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

CHAPTER 1

PPP in Subscriber Access Networks

Subscriber Access Overview

The Juniper Networks Junos OS subscriber access feature provides subscriber access, authentication, and service creation, activation, and deactivation. You can also collect accounting information and statistics for subscriber service sessions.

The subscriber access feature supports both CLI and AAA-based configuration (such as RADIUS) for subscribers. Access and services start when the router receives a message from a client (such as a DHCP discover message). For RADIUS clients, RADIUS Access-Accept messages and Change-of-Authorization-Request (CoA-Request) messages can create, modify, and delete subscriber sessions as well as activate and deactivate service sessions. You can use CLI commands to create a dynamic profile, which acts as a template of user attributes.

A subscriber service is based on the combination of a defined dynamic profile and attributes configured through authentication. Dynamic profiles can include dynamic firewall filters, class-of-service (CoS) settings, and protocol (IGMP) settings that define access limits for subscribers and the scope of a service granted to the subscriber after access is obtained.

The subscriber access feature provides the following convenience and flexibility to service providers and subscribers:

- Service providers can separate services and access technology and eliminate unprofitable flat-rate billing. They gain the ability to efficiently design, manage, and deliver services that subscribers want, and then bill subscribers based on connect time, bandwidth, and the actual service used.
- Subscribers benefit by gaining access to multiple simultaneous services. Depending on the service provider configuration, subscribers can dynamically connect to and disconnect from various services when they want and for however long they want. Subscribers can be billed based on the service level and usage, rather than being charged a set rate regardless of usage.

Subscriber Access Terms and Acronyms

Table 3 on page 4 defines terms and acronyms that are used in this discussion of subscriber access.

Table 3: Subscriber Access Terms and Acronyms

Term	Definition
AAA method for subscriber authentication	The AAA method that uses authentication (for example, including RADIUS VSAs in the Access-Accept packet) to verify a subscriber and activate a service when the subscriber logs in.
Dynamic profile	A template that defines a set of characteristics that are combined with authorization attributes and are dynamically assigned to static interfaces to provide dynamic subscriber access and services for broadband applications.
RADIUS CoA method	The method that uses RADIUS CoA-Request messages and VSAs to activate a service for a subscriber that is already logged in.
Subscriber access technology	The technology used by a subscriber to access services (for example, DHCP).

Related Documentation

- *Subscriber Access Environment*
- *Subscriber Access Licensing Overview*
- *Subscriber Access Operation Flow Using DHCP Relay*
- Configuring Subscriber Access on page 10

Subscriber Activation and Service Management in an Access Network

The subscriber access feature uses dynamic profiles to activate subscribers and manage services.

A dynamic profile is a set of characteristics, defined in a template, that the router uses to provide dynamic subscriber access and services.

By using dynamic profiles you can:

- Define access for your network
- Define different service levels for subscribers
- Preprovision services that you can activate later

Using AAA-based login (RADIUS-based login or RADIUS CoA) you can:

- Provide subscribers with dynamic activation and deactivation based on service selection
- Provide greater flexibility and efficient management for a large number of subscribers and services

Components of a Dynamic Profile

You can use dynamic profiles to define various router components for subscriber access.

These components include the following:

- Dynamic firewall filters—Includes input and output filters to enforce rules that define whether to permit or deny packets that are transmitting an interface on the router. To apply dynamic firewall filters to the subscriber interface, you configure static input and output firewall filters and reference those filters in dynamic profiles.
- Dynamic Class of Service (CoS)—Includes CoS values that define a service for a subscriber. For example, you can configure the shaping rate for traffic in a video service by referencing CoS statements in a dynamic profile.
- Dynamic signaling protocol—Includes dynamic IGMP configuration for host to router signaling for IPv4 to support IP multicasting.

Router Predefined Variables Used by Dynamic Profiles

The router contains many predefined variables. These variables enable dynamic association of certain interface-specific values to incoming subscriber requests. You must specify these predefined variables in certain statements within a dynamic profile. When a client accesses the router, the dynamic profile configuration replaces the predefined variable with the actual data from an incoming client data packet and configuration (local and RADIUS).

Related Documentation

- *Dynamic Profiles Overview*
- *Subscriber Interface Overview*
- *Junos OS Predefined Variables*

Dynamic Profiles for PPP Subscriber Interfaces Overview

Subscriber management PPP support enables you to create and attach dynamic profiles for PPP subscriber interfaces. When the PPP subscriber logs in, the router instantiates the specified dynamic profile and then applies the attributes defined in the profile to the interface.

Dynamic profiles are used for both static and dynamic PPP interfaces. For static PPP interfaces, you use the CLI to attach dynamic profiles, which specify PPP options. For dynamic PPP interfaces, the dynamic profile creates the interface, including the PPP options.

NOTE: **Dynamically created interfaces are supported only on PPPoE interfaces.**

Unlike traditional PPP support, subscriber management does not allow bi-directional PPP authentication—authentication is performed only by the router, never by the remote

peer. The router's AAA process manages authentication and address assignment for subscriber management. When you configure PPP options for a dynamic profile, you can configure either Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication, and you can control the order in which the router negotiates the CHAP and PAP protocols. In addition, for CHAP authentication, you can modify the default length of the CHAP challenge message. Other PPP options, which are either commonly used or mandatory for a traditional PPP interface configuration, are not supported in subscriber management dynamic profiles.

Related Documentation

- Configuring Dynamic Authentication for PPP Subscribers on page 17
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 24
- Verifying and Managing PPP Configuration for Subscriber Management on page 57
- Example: Minimum PPPoE Dynamic Profile on page 27

PART 2

Configuration

CHAPTER 2

Configuration Overview

Configuring Dynamic Profiles for PPP

A dynamic profile acts as a template that enables you to create, update, or remove a configuration that includes attributes for client access (for example, interface or protocol) or service (for example, IGMP). Using these profiles you can consolidate all of the common attributes of a client (and eventually a group of clients) and apply the attributes simultaneously.

After they are created, the profiles reside in a profile library on the router. You can then use the **dynamic-profile** statement to attach profiles to interfaces. To assign a dynamic profile to a PPP interface, you can include the **dynamic-profile** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* ppp-options]** hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number ppp-options]
dynamic-profile profile-name;
```

To monitor the configuration, issue the **show interfaces *interface-name*** command.

For information about dynamic profiles, see *Dynamic Profiles Overview* in the *Junos Subscriber Access Configuration Guide*.

For information about creating dynamic profiles, see *Configuring a Basic Dynamic Profile* in the *Junos Subscriber Access Configuration Guide*.

For information about assigning a dynamic profile to a PPP interface, see "Attaching Dynamic Profiles to Static PPP Subscriber Interfaces" on page 24 in the *Junos Subscriber Access Configuration Guide*.

NOTE: Dynamic profiles for PPP subscribers are supported only on PPPoE interfaces for this release.

Related Documentation

- Configuring Dynamic Authentication for PPP Subscribers on page 17

Configuring Subscriber Access

To configure subscriber access:

1. Configure the client access protocol.
   - Configure DHCP local server.

     See *Extended DHCP Local Server Overview*.
   - Configure DHCP relay.

     See *Extended DHCP Relay Agent Overview*.
   - Configure PPP.

     See *Configuring Logical Interface Properties* and *Configuring PPPoE*
2. Configure subscriber authentication, accounting, and addressing.
   a. Configure RADIUS:
      1. Specify the RADIUS servers.

         See *Specifying RADIUS Authentication and Accounting Servers for Subscriber Access*.
      2. Specify any optional server attributes.

         See *Configuring RADIUS Server Options for Subscriber Access*.
      3. (Optional) Configure the CoA feature for the RADIUS dynamic-request server to change or deactivate the service after login.

         See *Configuring RADIUS-Initiated Dynamic Request Support*.
      4. Configure subscriber accounting (RADIUS accounting).

         See *Configuring Per-Subscriber Session Accounting*.

   b. Configure addressing:
      - See *Configuring Address-Assignment Pools*.
3. Create and manage dynamic profiles for access and service.
   a. Configure a basic dynamic profile.

      See *Configuring a Basic Dynamic Profile*.

      See "Example: Minimum PPPoE Dynamic Profile" on page 27
   b. Configure a dynamic profile for access.

      See *Configuring a Dynamic Profile for DHCP Client Access*.
   c. Configure a dynamic profile for services.

      See *Configuring a Dynamic Profile for Various Levels of Services*.
   d. Configure a default subscriber service.

See *Configuring a Default Subscriber Service*.

e. Configure the static subscriber interfaces to be referenced in the dynamic profile.

See *Configuring a Subscriber Interface with a Static VLAN Interface*.

f. Specify the interface-name and unit variables that the router uses to dynamically associate to a subscriber's incoming interface.

See *Associating Dynamic Profiles with Statically Created Interfaces*.

g. Add, modify, or delete dynamic profile values to manage subscriber access and services.

See *Modifying Dynamic Profiles with Versioning Disabled*.

The router dynamically activates or modifies the subscriber service using the RADIUS configuration.

- When the subscriber logs in, the router dynamically activates the service.

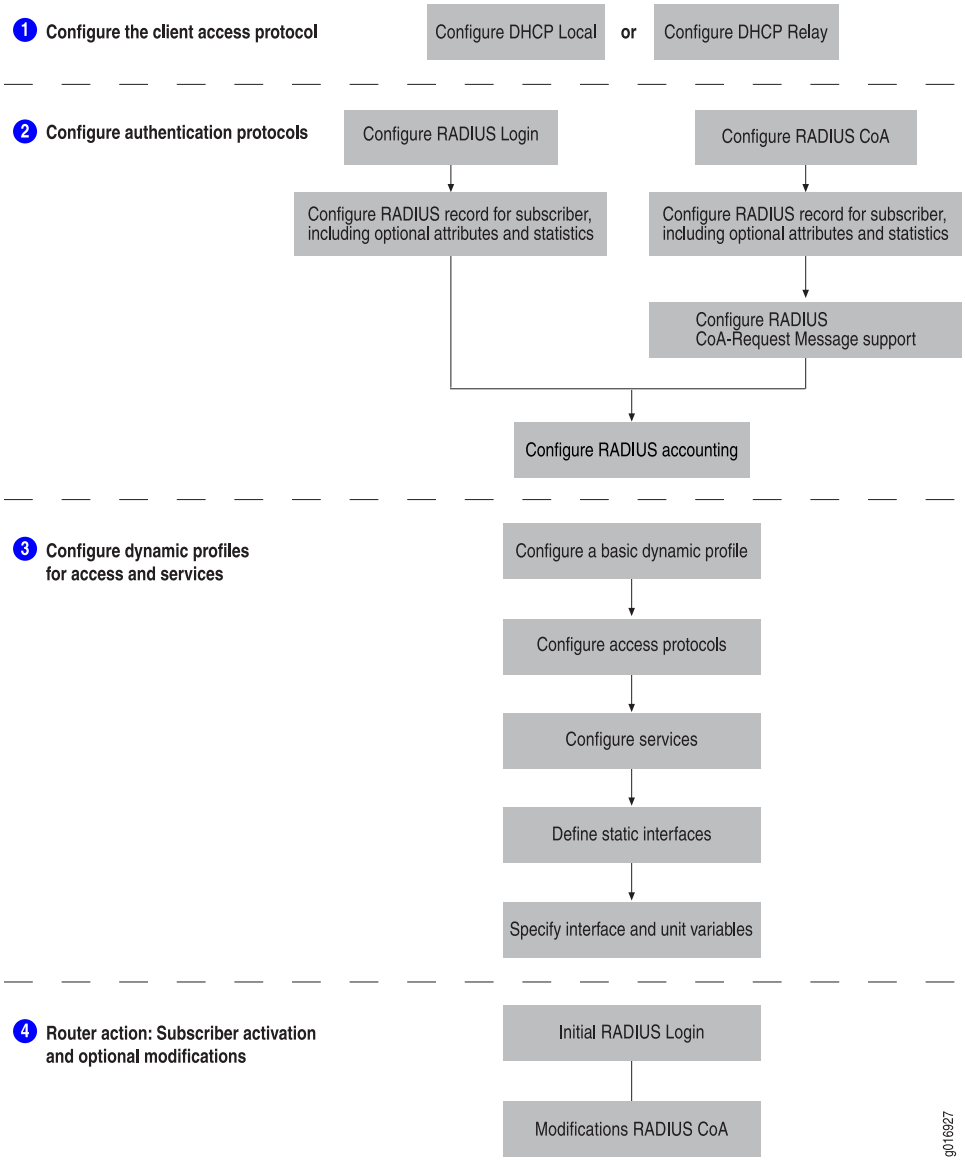
  See *Dynamic Service Activation During Login Overview*.

- If RADIUS CoA has been configured, the router can dynamically modify the service for a subscriber.

  See *RADIUS-Initiated Change of Authorization (CoA) Overview*.

Figure 1 on page 12 shows the configuration sequence you perform for DHCP-based subscriber access. It also shows the dynamic configuration performed by the router.

Figure 1: Subscriber Access Configuration Workflow



Related Documentation

- Subscriber Access Overview on page 3
- *Subscriber Access Support Considerations*
- *Default Subscriber Service Overview*
- *CLI-Activated Subscriber Services*

PPP Network Control Protocol Negotiation Mode Overview

The *Network Control Protocol* (NCP) is a mechanism used to establish and configure different Network Layer protocols for Point-to-Point Protocol (PPP) connections. On MX Series routers with Modular Port Concentrators (MPCs), you can configure *PPP NCP negotiation* to actively or passively control subscriber connections initiated by the router functioning as a PPP server.

PPP NCP Negotiation Modes

PPP NCP negotiation operates in either of the following modes:

- *Active PPP NCP negotiation mode*—The router sends an NCP Configuration Request message without waiting for the PPP client to do so.
- *Passive PPP NCP negotiation mode*—The router waits for the PPP client to send an NCP Configuration Request message before sending its own Configuration Request message. Dynamic subscriber interface connections and static subscriber interface connections use passive PPP NCP negotiation by default.

Router behavior for active mode and passive mode PPP NCP negotiation differs for dynamic PPP subscribers and static PPP subscribers, as summarized in Table 4 on page 13.

Table 4: PPP NCP Negotiation Mode Behavior for Dynamic and Static Subscribers

PPP Subscribers	PPP NCP Negotiation Mode	Router Behavior
Dynamic	Active	The router establishes the local network address and uses it to send the NCP Configuration Request message without waiting for the PPP client to send a Configuration Request.
Dynamic	Passive	The router establishes the local network address after it receives the NCP Configuration Request message from the PPP client.

Table 4: PPP NCP Negotiation Mode Behavior for Dynamic and Static Subscribers *(continued)*

PPP Subscribers	PPP NCP Negotiation Mode	Router Behavior
Static	Active	The router sends the authentication acknowledgement to the PPP client, and then sends the NCP Configuration Request message without waiting for the PPP client to send its own Configuration Request.
Static	Passive	The router sends the authentication acknowledgement to the PPP client, and then waits for an NCP Configuration Request message from the client before sending a Configuration Request.

PPP NCP Negotiation Mode Supported Configurations

You can configure PPP Network Control Protocol (NCP) negotiation for the following single-stack and dual-stack subscriber configurations on MX Series routers with MPCs:

- Dynamic PPP subscriber connections terminated at the router
- Static PPP subscriber connections terminated at the router
- Dynamic tunneled PPP subscribers at the L2TP network server (LNS)
- Static tunneled PPP subscribers at the L2TP network server (LNS) on an inline service (**si**) interface

PPP NCP Active Negotiation Requirements for IPv4 Dynamic and Static PPP Subscribers

To configure active PPP IPv4 Network Control Protocol (IPNCP) negotiation for dynamic and static PPP subscribers in a single-stack or dual-stack configuration, make sure you meet the following requirements:

- Configure the IPv4 (**inet**) protocol family in a dynamic profile (for dynamic subscribers) or at the interface level (for static subscribers).
- Assign any of the following IPv4 address attributes for the subscriber during the authentication process:
  - Framed-IP-Address (RADIUS Attribute 8)—RADIUS explicit IPv4 address
  - Framed-Pool (RADIUS Attribute 88)—RADIUS IPv4 adress pool name
  - IPv4 attributes allocated from a locally configured address pool

When you have met these requirements, use the **initiate-ncp ip** statement to enable active IPNCP negotiation for dynamic and static subscribers in a single-stack or dual-stack configuration.

PPP NCP Active Negotiation Requirements for IPv6 Dynamic and Static PPP Subscribers

To configure active PPP IPv6 Network Control Protocol (IPv6NCP) negotiation for dynamic and static PPP subscribers in a single-stack or dual-stack configuration, make sure you meet the following requirements:

- Configure the IPv6 (**inet6**) protocol family in a dynamic profile (for dynamic subscribers) or at the interface level (for static subscriber).
- Assign any of the following IPv6 address attributes for the subscriber during the authentication process:
  - Delegated-IPv6-Prefix (RADIUS Attribute 123)—RADIUS explicit IPv6 address
  - Framed-IPv6-Prefix (RADIUS Attribute 97)—RADIUS explicit IPv6 prefix
  - Framed-IPv6-Pool (RADIUS Attribute 100)—RADIUS explicit IPv6 adress or prefix pool name
  - IPv6 attributes allocated from a locally configured Neighbor Discovery Router Advertisement (NDRA) pool

When you have met these requirements, use the **initiate-ncp ipv6** statement to enable active IPv6NCP negotiation for dynamic and static subscribers in a single-stack or dual-stack configuration.

PPP NCP Negotiation Requirements for IPv4 and IPv6 Dual-Stack Configurations

You can configure either active or passive PPP NCP negotiation for the IPv4 and IPv6 subscriber interfaces in a dual-stack configuration.

To configure active negotiation in a dual-stack configuration, do all of the following:

- Make sure you meet the IPv4 and IPv6 protocol and address family requirements.
- Use the **initiate-ncp ip** statement to enable active negotiation for the IPv4 subscriber interface.
- Use the **initiate-ncp ipv6** statement to enable active negotiation for the IPv6 subscriber interface.

To configure passive negotiation in a dual-stack configuration, do both of the following:

- Make sure you meet the IPv4 and IPv6 protocol and address family requirements.
- Use the **initiate-ncp dual-stack-passive** statement to enable passive negotiation for the dual-stack configuration. The **initiate-ncp dual-stack-passive** statement overrides the **initiate-ncp ip** and **initiate-ncp ipv6** statements if they are configured.

The following additional guidelines apply when you configure PPP NCP negotiation for dual-stack subscribers:

- Dual-stack subscribers configured for either active mode or passive mode PPP NCP negotiation continue to use the same negotiation mode when the NCP mechanism is renegotiated.

- Using the **on-demand-ip-address** statement to save IPv4 addresses for dual-stack PPP subscribers when you are not using the IPv4 service has no effect on configuration of the PPP NCP negotiation mode in a dual-stack configuration.

Related Documentation

- Configuring the PPP Network Control Protocol Negotiation Mode on page 21

CHAPTER 3

Configuration Tasks for PPP Subscriber Access

Configuring Dynamic Authentication for PPP Subscribers

You can configure a dynamic profile that includes PPP authentication that enables PPP clients to dynamically access the network. You can specify either CHAP or PAP authentication. Optionally, you can also control the order in which the router negotiates the CHAP and PAP protocols.

For dynamic interfaces, the router supports unidirectional authentication only—the router always functions as the authenticator. When you configure PPP authentication in a dynamic profile, CHAP authentication supports the **challenge-length** option, which enables you to configure the minimum length and maximum length of the CHAP challenge message. Neither CHAP authentication nor PAP authentication supports any other configuration options, including the **passive** statement.

NOTE: **Dynamic profiles for PPP subscribers are supported only on PPPoE interfaces.**

To configure authentication in a dynamic profile for PPP subscriber interfaces:

1. Name the dynamic profile.

   ```
   [edit]
   user@host# edit dynamic-profiles vod-profile-25
   ```

2. Configure the interfaces and unit for the dynamic profile. Use **pp0** for the interface type and the Junos predefined variable for the unit.

```
[edit dynamic-profiles vod-profile-25]
user@host# edit interfaces pp0 unit $junos-interface-unit
```

3. Configure PPP options.

```
[edit dynamic-profiles vod-profile-25 interfaces pp0 unit "$junos-interface-unit"]
user@host# edit ppp-options
```

4. Specify the authentication protocol used in the dynamic profile. You can configure either CHAP or PAP. There are no additional options for either authentication protocol.

```
[edit dynamic-profiles vod-profile-25 interfaces pp0 unit "$junos-interface-unit"
  ppp-options]
user@host# set chap
```

5. (Optional) Configure the minimum length and maximum length of the CHAP challenge message.

   See "Modifying the CHAP Challenge Length" on page 22.

6. (Optional) Configure the order in which the router negotiates the CHAP and PAP authentication protocols.

   See "Controlling the Negotiation Order of PPP Authentication Protocols" on page 19.

Related Documentation

- Modifying the CHAP Challenge Length on page 22
- Controlling the Negotiation Order of PPP Authentication Protocols on page 19
- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 5
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 24
- *Dynamic Profiles Overview*
- *Configuring a Basic Dynamic Profile*
- Example: Minimum PPPoE Dynamic Profile on page 27
- Verifying and Managing PPP Configuration for Subscriber Management on page 57

Controlling the Negotiation Order of PPP Authentication Protocols

You can control the order in which the router tries to negotiate PPP authentication protocols when it verifies that a PPP client can access the network. By default, the router first tries to negotiate Challenge Handshake Authentication Protocol (CHAP) authentication. If the the attempt to negotiate CHAP authentication is unsuccessful, the router then tries to negotiate Password Authentication Protocol (PAP) authentication.

You can modify this default negotiation order in any of the following ways:

- Specify that the router negotiate PAP authentication first, followed by CHAP authentication if PAP negotiation is unsuccessful.

  When you specify both authentication protocols in either order, you must enclose the set of protocol names in square brackets ([ ]).

- Specify that the router negotiate only CHAP authentication.
- Specify that the router negotiate only PAP authentication.

Before you begin:

- Configure the CHAP or PAP protocol on the interface.
  - For dynamic PPP subscriber interfaces, see "Configuring Dynamic Authentication for PPP Subscribers" on page 17.
  - For CHAP on static interfaces with PPP encapsulation, see *Configuring the PPP Challenge Handshake Authentication Protocol*.
  - For PAP on static interfaces with PPP encapsulation, see *Configuring the PPP Password Authentication Protocol*.

To control the order in which the router negotiates PPP authentication protocols:

1. Specify that you want to configure PPP options.
   - For dynamic PPP subscriber interfaces:

     [edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit"]
     user@host# **edit** ppp-options

   - For static interfaces with PPP encapsulation:

     [edit interfaces pp0 unit *logical-unit-number*]
     user@host# **edit ppp-options**

2. Specify the negotiation order for PPP authentication protocols on the router.
   - For dynamic PPP subscriber interfaces:

     [edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit" ppp-options]
     user@host# **set** authentication **[*authentication-protocols*]**

   - For static interfaces with PPP encapsulation:

     [edit interfaces pp0 unit *logical-unit-number* ppp-options]

user@host# **set** authentication **[***authentication-protocols***]**

The following sample **authentication** statements in a dynamic profile named pppoe-client-profile show the different ways you can configure the negotiation order for PPP authentication protocols. (The **authentication** statements for configuring static interfaces are identical.)

- To specify that the router negotiate PAP authentication first, followed by CHAP authentication:

  ```
  [edit dynamic-profiles pppoe-client-profile interfaces pp0 unit "$junos-interface-unit"
    ppp-options]
  user@host# set authentication [pap chap]
  ```

- To specify that the router negotiate only CHAP authentication:

  ```
  [edit dynamic-profiles pppoe-client-profile interfaces pp0 unit "$junos-interface-unit"
    ppp-options]
  user@host# set authentication chap
  ```

- To specify that the router negotiate only PAP authentication:

  ```
  [edit dynamic-profiles pppoe-client-profile interfaces pp0 unit "$junos-interface-unit"
    ppp-options]
  user@host# set authentication pap
  ```

- To restore the default negotiation order for PPP authentication protocols after you have modified it:

  ```
  [edit dynamic-profiles pppoe-client-profile interfaces pp0 unit "$junos-interface-unit"
    ppp-options]
  user@host# set authentication [chap pap]
  ```

Related Documentation

- Configuring Dynamic Authentication for PPP Subscribers on page 17
- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 5
- *Configuring the PPP Challenge Handshake Authentication Protocol*
- *Configuring the PPP Password Authentication Protocol*

Configuring the PPP Network Control Protocol Negotiation Mode

Configuring PPP Network Control Protocol (NCP) negotiation enables you to actively or passively control subscriber connections initiated by the router functioning as a PPP server. Both dynamic and static subscriber interface connections use passive PPP NCP negotiation by default.

You can configure the PPP NCP negotiation mode (active or passsive) for the following subscriber configurations on MX Series routers with MPCs:

- Dynamic PPP subscriber connections terminated at the router, using a dynamic profile
- Static PPP subscriber connections terminated at the router, using a per-interface configuration
- Dynamic tunneled PPP subscribers at the L2TP network server (LNS), using a dynamic profile
- Static tunneled PPP subscribers at the LNS, using a per-inline service (**si**) interface configuration
- Dynamic and static tunneled PPP subscribers at the LNS, using a user-group profile

To configure PPP NCP negotiation mode:

1. Specify that you want to configure PPP-specific properties for the subscriber.
   - For dynamic PPP subscriber connections terminated at the router:

     [edit dynamic-profiles *profile-name* interfaces pp0 unit “$junos-interface-unit”]
     user@host# **edit ppp-options**
   - For static PPP subscriber connections terminated at the router:

     [edit interfaces pp0 unit *logical-unit-number*]
     user@host# **edit ppp-options**
   - For dynamic tunneled PPP subscribers at the LNS:

     [edit dynamic-profiles *profile-name* interfaces “$junos-interface-ifd-name” unit “$junos-interface-unit”]
     user@host# **edit ppp-options**
   - For static tunneled PPP subscribers at the LNS:

     [edit interfaces si-*fpc/pic/port* unit *logical-unit-number*]
     user@host# **edit ppp-options**
   - In a group profile for dynamic and static tunneled PPP subscribers at the LNS:

     [edit access group-profile *profile-name* ppp]
     user@host# **edit ppp-options**
2. Configure PPP NCP negotiation mode in any of the following ways:
   - To configure active PPP NCP negotiation for IPv4 subscribers in a single-stack or dual-stack configuration, use the **initiate-ncp ip** statement.

For example, to configure active negotiation for static IPv4 connections terminated at the router:

```
[edit interfaces pp0 unit logical-unit-number ppp-options]
user@host# initiate-ncp ip
```

- To configure active PPP NCP negotiation for IPv6 subscribers in a single-stack or dual-stack configuration, use the **initiate-ncp ipv6** statement.

  For example, to configure active negotiation for dynamic IPv6 connections terminated at the router:

  ```
  [edit dynamic-profiles profile-name interfaces pp0 unit "$junos-interface-unit"
    ppp-options]
  user@host# initiate-ncp ipv6
  ```

- To configure passive PPP NCP negotiation for dynamic or static subscribers in an IPv4 and IPv6 dual-stack configuration, use the **initiate-ncp dual-stack-passive** statement, which overrides both the **initiate-ncp ip** and **initiate-ncp ipv6** statements if they are configured.

  For example, to configure passive negotiation for dynamic tunneled PPP subscribers at the LNS in an IPv4 and IPv6 dual-stack configuration:

  ```
  [edit dynamic-profiles profile-name interfaces "$junos-interface-ifd-name" unit
    "$junos-interface-unit"]
  user@host# initiate-ncp dual-stack-passive
  ```

Related Documentation

- PPP Network Control Protocol Negotiation Mode Overview on page 13

Modifying the CHAP Challenge Length

You can modify the default minimum length and maximum length of the Challenge Handshake Authentication Protocol (CHAP) challenge message that the router sends to a PPP client. The CHAP challenge message, which contains information that is unique to a particular PPP subscriber session, is used as part of the authentication mechanism between the router and the client to verify the identity of the client for access to the router.

By default, the minimum length of the CHAP challenge is 16 bytes, and the maximum length is 32 bytes. You can override this default to configure the CHAP challenge minimum length and maximum length in the range 8 bytes through 63 bytes.

BEST PRACTICE: **We recommend that you configure both the minimum length and the maximum length of the CHAP challenge to at least 16 bytes.**

Before you begin:

- Configure the CHAP protocol on the interface.
  - For dynamic PPP subscriber interfaces, see "Configuring Dynamic Authentication for PPP Subscribers" on page 17.

- For static interfaces with PPP encapsulation, see *Configuring the PPP Challenge Handshake Authentication Protocol*.

To configure the minimum and maximum length of the CHAP challenge message:

1. Specify that you want to configure PPP options.
   - For dynamic PPP subscriber interfaces:

     [edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit"]
     user@host# **edit** ppp-options
   - For static interfaces with PPP encapsulation:

     [edit interfaces pp0 unit *logical-unit-number*]
     user@host# **edit ppp-options**
2. Specify that you want to configure CHAP options.
   - For dynamic PPP subscriber interfaces:

     [edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit" ppp-options]
     user@host# **edit** chap
   - For static interfaces with PPP encapsulation:

     [edit interfaces pp0 unit *logical-unit-number* ppp-options]
     user@host# **edit chap**
3. Specify the minimum length and maximum length of the CHAP challenge.
   - For dynamic PPP subscriber interfaces:

     [edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit" ppp-options chap]
     user@host# **set** challenge-length **minimum** *minimum-length* **maximum** *maximum-length*
   - For static interfaces with PPP encapsulation:

     [edit interfaces pp0 unit *logical-unit-number* ppp-options chap]
     user@host# **set** challenge-length **minimum** *minimum-length* **maximum** *maximum-length*

   For example, the following **challenge-length** statement in a dynamic profile named pppoe-client-profile sets the minimum length of the CHAP challenge to 20 bytes, and the maximum length to 40 bytes.

   [edit dynamic-profiles pppoe-client-profile interfaces pp0 unit "$junos-interface-unit" ppp-options chap]
   user@host# **set challenge-length minimum 20 maximum 40**

Related Documentation

- Configuring Dynamic Authentication for PPP Subscribers on page 17
- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 5
- *Configuring the PPP Challenge Handshake Authentication Protocol*

Attaching Dynamic Profiles to Static PPP Subscriber Interfaces

You can attach a dynamic profile to a static PPP subscriber interface. When a PPP subscriber logs in, the specified dynamic profile is instantiated and the services defined in the profile are applied to the interface.

To attach a dynamic profile to a static PPP subscriber interface:

1. Specify that you want to configure PPP options.

   ```
   [edit interfaces pp0 unit 0]
   user@host# edit ppp-options
   ```

2. Specify the dynamic profile you want to associate with the interface.

   ```
   [edit interfaces pp0 unit 0 ppp-options]
   user@host# set dynamic-profile vod-profile-50
   ```

Related Documentation

- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 5
- Configuring Dynamic Authentication for PPP Subscribers on page 17
- *Dynamic Profiles Overview*
- *Configuring a Basic Dynamic Profile*
- Example: Minimum PPPoE Dynamic Profile on page 27
- Verifying and Managing PPP Configuration for Subscriber Management on page 57

Understanding How the Router Processes Subscriber-Initiated PPP Fast Keepalive Requests

On MX Series routers with Modular Port Concentrators/Modular Interface Cards (MPCs/MICs), the Packet Forwarding Engine on an MPC/MIC processes and responds to Link Control Protocol (LCP) Echo-Request packets that the PPP subscriber (client) initiates and sends to the router. LCP Echo-Request packets and LCP Echo-Reply packets are part of the PPP keepalive mechanism that helps determine whether a link is functioning properly.

Previously, LCP Echo-Request packets and LCP Echo-Reply packets were handled on an MX Series router by the Routing Engine. Support for the PPP fast keepalive feature enables the Packet Forwarding Engine on the MPC/MIC to receive LCP Echo-Request packets from the PPP subscriber and transmit LCP Echo-Reply packets in response, without having to send the LCP packets to the Routing Engine for processing. The mechanism by which LCP Echo-Request packets are processed by the Packet Forwarding Engine instead of by the Routing Engine is referred to as *PPP fast keepalive*.

Relieving the Routing Engine of having to process LCP Echo-Request packets provides increased bandwidth on the router to support a larger number of subscribers with improved performance.

How PPP Fast Keepalive Processing Works

You do not need any special configuration on an MX Series router with MPCs/MICs to enable processing of PPP fast keepalive requests on the Packet Forwarding Engine. The feature is enabled by default, and cannot be disabled.

The following sequence describes how an MX Series router processes LCP Echo-Request packets and LCP Echo-Reply packets on the Packet Forwarding Engine on the MPC/MIC:

1. The Routing Engine notifies the Packet Forwarding Engine when transmission of keepalive requests is enabled on a PPP logical interface. The notification includes the magic numbers of both the server and the remote client.
2. The Packet Forwarding Engine receives the LCP Echo-Request packet initiated by the PPP subscriber (client).
3. The Packet Forwarding Engine validates the peer magic number in the LCP Echo-Request packet, and transmits the corresponding LCP Echo-Reply packet containing the magic number negotiated by the router.
4. If the Packet Forwarding Engine detects a loop condition in the link, it sends the LCP Echo-Request packet to the Routing Engine for further processing.

   The Routing Engine continues to process LCP Echo-Request packets until the loop condition is cleared.

Transmission of keepalive requests from the Packet Forwarding Engine on the router is not currently enabled.

Statistics Display for PPP Fast Keepalive

When an MX Series router with MPCs/MICs is using PPP fast keepalive for a PPP link, the **Keepalive statistics** field in the output of the **show interfaces pp0.*logical* statistics** operational command does not include statistics for the number of keepalive packets received or sent, or the amount of time since the router received or sent the last keepalive packet.

Effect of Changing the Forwarding Class Configuration

To change the default queue assignment (forwarding class) for outbound traffic generated by the Routing Engine, you can include the **forwarding-class *class-name*** statement at the **[edit class-of-service host-outbound-traffic]** hierarchy level.

For PPP fast (inline) keepalive LCP Echo-Request and LCP Echo-Reply packets transmitted between an MX Series router with MPCs/MICs and a PPP client, changing the forwarding class configuration takes effect immediately for both new PPP-over-Ethernet (PPPoE), PPP-over-ATM (PPPoA), and L2TP network server (LNS) subscriber sessions created after the configuration change, and for existing PPPoE, PPPoA, and LNS subscriber sessions established before the configuration change.

Related Documentation

- *Configuring Keepalives*
- *Disabling the Sending of PPPoE Keepalive Messages*
- *Changing the Default Queuing and Marking of Host Outbound Traffic*

CHAPTER 4

Examples

Example: Minimum PPPoE Dynamic Profile

This example shows the minimum configuration for a dynamic profile that is used for static PPPoE interfaces. The configuration must include the **interfaces pp0** stanza.

```
dynamic-profiles {
   ppp-profile-1 {
      interfaces {
         pp0 {
            unit "$junos-interface-unit";
         }
      }
   }
}
```

Related Documentation

- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 5
- Configuring Dynamic Authentication for PPP Subscribers on page 17
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 24

CHAPTER 5

Configuration Statements

[edit protocols ppp-service] Hierarchy Level

The following statement hierarchy can also be included at the **[edit logical-systems *logical-system-name*]** hierarchy level.

```
protocols {
  ppp-service {
    on-demand-ip-address;
    reject-unauthorized-ipv6cp;
    traceoptions {
      file filename <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
      filter {
        aci regular-expression;
        ari regular-expresion;
        service-name regular-expresion;
        underlying-interface interface-name;
        user user@domain;
      }
      flag flag;
      level severity;
      no-remote-trace;
    }
  }
}
```

Related Documentation

- *Notational Conventions Used in Junos OS Configuration Hierarchies*
- *[edit protocols] Hierarchy Level*

address-change-immediate-update

Syntax address-change-immediate-update;

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 13.1.

Description Configure the router to send an Address-Change-Update message to the RADIUS accounting server. Any change to this setting takes effect for all new subscriber logins. Existing subscribers are not impacted by this change except when the AAA daemon restarts.

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

Related Documentation

- *Saving IPv4 Addresses for Dual-Stack PPP Subscribers*

authentication (Static and Dynamic PPP)

Syntax authentication [*authentication-protocols*];

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit" ppp-options], [edit interfaces pp0 unit *unit-number* ppp-options]

Release Information Statement introduced in Junos OS Release 12.2.

Description Specify the order in which the router tries to negotiate PPP authentication protocols when verifying that a PPP client can access the network. By default, the router tries to negotiate Challenge Handshake Authentication Protocol (CHAP) authentication first, and then tries Password Authentication Protocol (PAP) authentication if the attempt to negotiate CHAP authentication is unsuccessful.

You can specify one or both authentication protocols. If you specify both CHAP and PAP in either order, you must enclose the set of protocol names within square brackets ([ ]).

Options ***authentication-protocols***—One or both of the following PPP authentication protocols:

- **chap**—Challenge Handshake Authentication Protocol
- **pap**—Password Authentication Protocol

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

Related Documentation

- Controlling the Negotiation Order of PPP Authentication Protocols on page 19

challenge-length (Static and Dynamic PPP)

Syntax challenge-length minimum *minimum-length* maximum *maximum-length*;

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit" ppp-options chap],
[edit interfaces pp0 unit *unit-number* ppp-options chap]

Release Information Statement introduced in Junos OS Release 12.2.

Description Modify the length of the Challenge Handshake Authentication Protocol (CHAP) challenge by specifying the minimum and maximum allowable length, in bytes.

BEST PRACTICE: We recommend that you configure both the minimum length and the maximum length of the CHAP challenge to at least 16 bytes.

Options ***minimum-length***—Minimum length, in bytes, of the CHAP challenge.

Range: 8 through 63

Default: 16

maximum-length—Maximum length, in bytes, of the CHAP challenge. The *maximum-length* must be equal to or greater than the *minimum-length*.

Range: 8 through 63

Default: 32

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

Related Documentation

- Modifying the CHAP Challenge Length on page 22

chap (Dynamic PPP)

Syntax

```
chap {
  challenge-length minimum minimum-length maximum maximum-length;
}
```

Hierarchy Level

[edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit" ppp-options],
[edit dynamic-profiles *profile-name* interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" ppp-options]

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" ppp-options]** hierarchy level introduced in Junos OS Release 12.2.

Description

Specify CHAP authentication in a PPP dynamic profile.

The remaining statement is explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Dynamic Profiles Overview*
- Configuring Dynamic Authentication for PPP Subscribers on page 17
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 24
- *Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface*

dynamic-profile (PPP)

Syntax dynamic-profile *profile-name*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* ppp-options]

Release Information Statement introduced in Junos OS Release 9.5.
Support for MLPPP on LSQ interfaces introduced in Junos OS Release 10.2.

Description Specify the dynamic profile that is attached to the interface. On the MX Series routers, this statement is currently supported on PPPoE interfaces only. On the M120 and M320 routers, this statement is supported for MLPPP bundles only on LSQ interfaces on Adaptive Services PICs and Multiservices PICs.

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

Related Documentation

- *Dynamic Profiles Overview*
- *Configuring a Basic Dynamic Profile*
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 24
- *Attaching Dynamic Profiles to MLPPP Bundles*
- For hardware requirements, see *Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces*

ip-address-change-notify

Syntax ip-address-change-notify *message*;

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

Release Information Statement introduced in Junos OS Release 13.1.

Description Configure the Unisphere-IPv4-release-control VSA in RADIUS messages. When enabled, the BNG includes Unisphere-Ipv4-release-control VSA in the Access-Request that is sent during on-demand IP address allocation and in the immediate Interim-Accounting messages that are sent to report an address change. Disabled by default, there is no effect when on-demand IP address allocation or deallocation is not configured. An change takes effect immediately. It is optional to specify the message, but if specified, the message is inserted into Unisphere-Ipv4-release-control VSA. Otherwise, a default value (NO MESSAGE) is be inserted into the VSA.

Options ***message***—VSA message.

Range: 1 through 32 characters,

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

Related Documentation

- *Saving IPv4 Addresses for Dual-Stack PPP Subscribers*

initiate-ncp (Dynamic and Static PPP)

Syntax initiate-ncp (ip | ipv6 | dual-stack-passive);

Hierarchy Level
[edit access group-profile *profile-name* ppp ppp-options],
[edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit" ppp-options],
[edit dynamic-profiles *profile-name* interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" ppp-options],
[edit interfaces pp0 unit *logical-unit-number* ppp-options],
[edit interfaces si-*fpc/pic/port* unit *logical-unit-number* ppp-options]

Release Information Statement introduced in Junos OS Release 14.1.

Description Configure PPP Network Control Protocol (NCP) negotiation mode (active or passive) for dynamic and static IPv4 and IPv6 PPP subscriber interfaces. You can also configure PPP NCP negotiation mode for the PPP server in an IPv4/IPv6 dual-stack configuration.

Options

dual-stack-passive—Enable passive PPP NCP negotiation for the PPP server in an IPv4/IPv6 dual-stack configuration. The **initiate-ncp dual-stack-passive** statement overrides the **initiate-ncp ip** and **initiate-ncp ipv6** statements if they are configured in an IPv4/IPv6 dual-stack configuration.

ip—Enable active PPP NCP negotiation for dynamic and static PPP subscriber interfaces configured with the IPv4 (**inet**) protocol address family, and for which IPv4 address attributes are assigned during authorization. By default, dynamic and static IPv4 subscriber interfaces use passive PPP NCP negotiation. In an IPv4/IPv6 dual-stack configuration, use the **initiate-ncp ip** statement to enable active PPP NCP negotiation for the IPv4 subscriber interface.

ipv6—Enable active PPP NCP negotiation for dynamic and static PPP subscriber interfaces configured with the IPv6 (**inet6**) protocol address family, and for which IPv6 address attributes are assigned during authorization. By default, dynamic and static IPv6 subscriber interfaces use passive PPP NCP negotiation. In an IPv4/IPv6 dual-stack configuration, use the **initiate-ncp ipv6** statement to enable active PPP NCP negotiation for the IPv6 subscriber interface.

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

Related Documentation

- Configuring the PPP Network Control Protocol Negotiation Mode on page 21
- PPP Network Control Protocol Negotiation Mode Overview on page 13

keepalives (Dynamic Profiles)

Syntax

```
keepalives {
    interval seconds;
    }
```

Hierarchy Level

[edit dynamic-profiles *profile-name* interfaces pp0 unit *logical-unit-number*]
[edit dynamic-profiles *profile-name* interfaces pp0 unit “$junos-interface-unit”]
[edit dynamic-profiles *profile-name* interfaces "$junos-interface-ifd-name" unit “$junos-interface-unit”]

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* interfaces pp0 unit “$junos-interface-unit”]** hierarchy level introduced in Junos OS Release 10.1.
Support at the **[edit dynamic-profiles *profile-name* interfaces "$junos-interface-ifd-name" unit “$junos-interface-unit”]** hierarchy level introduced in Junos OS Release 12.2.

Description

Specify the keepalive interval in a PPP dynamic profile.

Default

Sending of keepalives is enabled by default.

Options

interval *seconds*—The time in seconds between successive keepalive requests.

Range: 1 through 32767 seconds

Default: 30 seconds for LNS-based PPP sessions. 10 seconds for all other PPP sessions.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Dynamic Profiles Overview*
- Configuring Dynamic Authentication for PPP Subscribers on page 17
- *Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface*

mac-address (Dynamic Access-Internal Routes)

Syntax mac-address *address*;

Hierarchy Level [edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access-internal route *subscriber-ip-address* qualified-next-hop *underlying-interface*],
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access-internal route *subscriber-ip-address* qualified-next-hop *underlying-interface*],
[edit dynamic-profiles routing-options access-internal route *subscriber-ip-address* qualified-next-hop *underlying-interface*]

Release Information Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options route *subscriber-ip-address* qualified-next-hop *underlying-interface*]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* route *subscriber-ip-address* qualified-next-hop *underlying-interface*]** hierarchy levels introduced in Junos OS Release 10.1.

Description Dynamically configure the MAC address variable for an access-internal route for unnumbered interfaces such as DHCP subscriber interfaces.

Options *address*—Either the specific MAC address you want to assign to the access-internal route or the MAC address variable ($junos-subscriber-mac-address). The MAC address variable is dynamically replaced with the value supplied by DHCP when a subscriber logs in.

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

Related Documentation
- *Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management*

metric (Dynamic Access-Internal Routes)

Syntax metric *route-cost*;

Hierarchy Level [edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*],
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*],
[edit dynamic-profiles *profile-name* routing-options access route *prefix*]

Release Information Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*]** hierarchy levels introduced in Junos OS Release 10.1.

Description Dynamically configure the cost for an access route.

Options *route-cost*—Either the specific cost you want to assign to the access route or either of the following cost variables:

- **$junos-framed-route-cost**—Cost of an IPv4 access route; the variable is dynamically replaced with the metric value (Subattribute 3) from the RADIUS Framed-Route attribute [22].
- **$junos-framed-route-ipv6-cost**—Cost of an IPv6 access route; the variable is dynamically replaced with the metric value (Subattribute 3) from the RADIUS Framed-IPv6-Route attribute [99].

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

Related Documentation
- *Configuring Dynamic Access Routes for Subscriber Management*

next-hop (Dynamic Access-Internal Routes)

Syntax next-hop *next-hop*;

Hierarchy Level [edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*],
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*],
[edit dynamic-profiles *profile-name* routing-options access route *prefix*]

Release Information Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*]** hierarchy levels introduced in Junos OS Release 10.1.

Description Dynamically configure the next-hop address for an access route. Access routes are typically unnumbered interfaces.

Options *next-hop*—Either the specific next-hop address you want to assign to the access route or one of the following next-hop address predefined variables.

- For IPv4 access routes, use the variable, **$junos-framed-route-nexthop**. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22].
- For IPv6 access routes, use the variable, **$junos-framed-route-ipv6-nexthop**. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].

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

Related Documentation
- *Configuring Dynamic Access Routes for Subscriber Management*

on-demand-ip-address

Syntax on-demand-ip-address;

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit" ppp-options],
[edit interfaces pp0 unit *unit-number* ppp-options],
[[edit protocols ppp-service] on page 29]

Release Information Statement introduced in Junos OS Release 13.1.

Description Allocates and de-allocates an IPv4 address after initial PPP authentication for a subscriber who does not have an existing IPv4 address and can be configured at either the interface level or at the system level. Disabled by default. When configured at the interface level, dynamic profile changes take effect only for any new subscriber logins. Changes for static PPP IFLs logs out the subscriber. When configured at the system level, globally enables an on-demand-ip-address for PPP subscribers. If configured at both the interface level and the system level, the system level configuration takes precedence and changes take effect only for new subscriber logins.

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

Related Documentation
- *Saving IPv4 Addresses for Dual-Stack PPP Subscribers*

pap (Dynamic PPP)

Syntax pap;

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces pp0 unit "$junos-interface-unit" ppp-options],
[edit dynamic-profiles *profile-name* interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" ppp-options]

Release Information Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" ppp-options]** hierarchy level introduced in Junos OS Release 12.2.

Description Specify PAP authentication in a PPP dynamic profile.

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

Related Documentation
- *Dynamic Profiles Overview*
- Configuring Dynamic Authentication for PPP Subscribers on page 17
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 24
- *Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface*

ppp-options (Dynamic PPP)

Syntax

```
ppp-options {
  authentication [ authentication-protocols ];
  chap {
    challenge-length minimum minimum-length maximum maximum-length;
  }
  initiate-ncp (ip | ipv6 | dual-stack-passive)
  on-demand-ip-address;
  pap;
}
```

Hierarchy Level

[edit dynamic-profiles *profile-name* interfaces pp0 unit “$junos-interface-unit”],
[edit dynamic-profiles *profile-name* interfaces "$junos-interface-ifd-name" unit “$junos-interface-unit”]

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* interfaces "$junos-interface-ifd-name" unit “$junos-interface-unit”]** hierarchy level introduced in Junos OS Release 12.2.

Description

Configure PPP-specific interface properties in a dynamic profile.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Dynamic Profiles Overview*
- Configuring Dynamic Authentication for PPP Subscribers on page 17
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 24
- *Applying PPP Attributes to L2TP LNS Subscribers Per Inline Service Interface*

preference (Subscriber Management)

Syntax preference *route-distance*

Hierarchy Level [edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*],
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*],
[edit dynamic-profiles *profile-name* routing-options access route *prefix*]

Release Information Statement introduced in Junos OS Release 9.5.
Support at **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*]** hierarchy levels introduced in Junos OS Release 10.1.

Description Dynamically configure the distance for an access route.

Options ***route-distance***—Either the specific distance you want to assign to the access route or either of the following distance variables:

- **$junos-framed-route-distance**—Distance of an IPv4 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-Route attribute [22].
- **$junos-framed-route-ipv6-distance**—Distance of an IPv6 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-IPv6-Route attribute [99].

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

Related Documentation
- *Configuring Dynamic Access Routes for Subscriber Management*

qualified-next-hop (Subscriber Management)

Syntax

```
qualified-next-hop interface-name {
    mac-address address;
}
```

Hierarchy Level

[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access-internal route *subscriber-ip-address*],
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access-internal route *subscriber-ip-address*],
[edit dynamic-profiles *profile-name* routing-options access-internal route *subscriber-ip-address*]

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options route *subscriber-ip-address*]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* route *subscriber-ip-address*]** hierarchy levels introduced in Junos OS Release 10.1.

Description

Dynamically configure the qualified next-hop and the MAC address for an access-internal route for DHCP and PPP subscriber interfaces.

Options

interface-name—Either the specific interface you want to assign to the access route or the variable, or the **$junos-interface-name** variable. The variable is dynamically replaced with the value supplied by DHCP or PPP when a subscriber logs in.

The remaining statement is 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 Dynamic Access-Internal Routes for DHCP Subscriber Management*

reject-unauthorized-ipv6cp

Syntax reject-unauthorized-ipv6cp;

Hierarchy Level [edit protocols ppp-service]

Release Information Statement introduced in Junos OS Release 13.3.

Description Configure the router to reject any IPv6 Control Protocol (IPv6CP) negotiation messages on dynamic interfaces when no appropriate IPv6 address or prefix has been received from AAA. IPv6CP negotiation attempts are also rejected when only a Framed-IPv6-Prefix attribute is received but router advertisement is not enabled in the dynamic profile.

NOTE: **IPv6CP negotiation messages are not rejected for static interfaces.**

Default IPv6CP negotiation is allowed regardless of the presence of IPv6 attributes received from AAA.

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

Related Documentation

- *Avoiding Negotiation of IPv6CP in the Absence of an Authorized Address*

route (Access)

Syntax

```
route prefix {
  next-hop next-hop;
  metric route-cost;
  preference route-distance;
  tag route-tag;
}
```

Hierarchy Level

[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access],
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access],
[edit dynamic-profiles *profile-name* routing-options access]

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access]** hierarchy levels introduced in Junos OS Release 10.1.

Description

Dynamically configure the parameters for access routes.

Options

prefix—Either the specific route prefix that you want to assign to the access route or one of the following route prefix variables.

- For IPv4 access routes, use the variable, **$junos-framed-route-ip-address-prefix**. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22].
- For IPv6 access routes, use the variable, **$junos-framed-route-ipv6-address-prefix**. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].

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 Dynamic Access Routes for Subscriber Management*

route (Access Internal)

Syntax

```
route subscriber-ip-address {
  next-hop next-hop;
  qualified-next-hop underlying-interface {
    mac-address address;
  }
}
```

Hierarchy Level

[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access-internal],
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access-internal],
[edit dynamic-profiles *profile-name* routing-options access-internal]

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access-internal]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access-internal]** hierarchy levels introduced in Junos OS Release 10.1.

Description

Dynamically configure parameters for an access-internal route.

Options

subscriber-ip-address—Either the specific IP address you want to assign to the access-internal route or the subscriber IP address variable ($junos-subscriber-ip-address). The subscriber IP address variable is dynamically replaced with the value supplied by DHCP or PPP when a subscriber logs in.

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 Dynamic Access-Internal Routes for DHCP Subscriber Management*
- *Configuring Dynamic Access-Internal Routes for PPP Subscriber Management*

routing-options (Dynamic Profiles)

Syntax

```
routing-options {
  access {
    route prefix {
      metric route-cost;
      next-hop next-hop;
      preference route-distance;
      tag route-tag;
    }
  }
  access-internal {
    route subscriber-ip-address {
      qualified-next-hop underlying-interface {
        mac-address address;
      }
    }
  }
  multicast {
    interface interface-name {
      no-qos-adjust;
    }
  }
  rib routing-table-name {
    access {
      route prefix {
        metric route-cost;
        next-hop next-hop;
        preference route-distance;
        tag route-tag;
      }
    }
    access-internal {
      route subscriber-ip-address {
        qualified-next-hop underlying-interface {
          mac-address address;
        }
      }
    }
  }
}
```

Hierarchy Level [edit dynamic-profiles *profile-name*],
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance]

Release Information Statement introduced in Junos OS Release 9.6.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance]** hierarchy level introduced in Junos OS Release 10.1.

Description Configure protocol-independent routing properties in a dynamic profile.

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 Dynamic Access Routes for Subscriber Management*
- *Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management*

tag (Access)

Syntax
tag *route-tag*;

Hierarchy Level
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*],
[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*],
[edit dynamic-profiles *profile-name* routing-options access route *prefix*]

Release Information
Statement introduced in Junos OS Release 10.2.
Support at the **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options access route *prefix*]** and **[edit dynamic-profiles *profile-name* routing-instances $junos-routing-instance routing-options rib *routing-table-name* access route *prefix*]** hierarchy levels introduced in Junos OS Release 10.1.

Description
Dynamically configure the tag for an access route.

Options
route-tag—Either the specific tag you want to assign to the access route or either of the following tag variables:

- **$junos-framed-route-tag**—Tag assigned to an IPv4 access route; the variable is dynamically replaced with the preference value (Subattribute 6) from the RADIUS Framed-Route attribute [22].
- **$junos-framed-route-ipv6-tag**—Tag assigned to an IPv6 access route; the variable is dynamically replaced with the preference value (Subattribute 6) from the RADIUS Framed-IPv6-Route attribute [99].

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

Related Documentation
- *Configuring Dynamic Access Routes for Subscriber Management*

traceoptions (Protocols PPP Service)

Syntax

```
traceoptions {
  file <filename> <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  filter {
    aci regular-expression;
    ari regular-expresion;
    service-name regular-expresion;
    underlying-interface interface-name;
    user user@domain;
  }
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level [edit protocols ppp-service]

Release Information Statement introduced in Junos OS Release 9.5.
Option **user** introduced in Junos OS Release 14.1.

Description Define tracing operations for PPP service processes.

Options

file *filename*—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**.

files *number*—(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.

Range: 2 through 1000

Default: 3 files

disable—Disable this trace flag.

filter—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifiers simplifies troubleshooting in a scaled environment.

BEST PRACTICE: Due to the complexity of agent circuit identifiers and agent remote identifiers, we recommend that you do not try an exact match when filtering on these options. For service names, searching on the exact name is appropriate, but you can also use a regular expression with that option.

- **aci** *regular-expression*—Regular expression to match the agent circuit identifier provided by PPP client.
- **ari** *regular-expression*—Regular expression to match the agent remote identifier provided by PPP client.

- **service** ***regular-expression***—Regular expression to match the name of PPPoE service.
- **underlying-interface** ***interface-name***—Name of a PPP underlying interface. You cannot use a regular expression for this filter option.
- **user** *user@domain*—Username of a subscriber. Optionally use an asterisk (*) as a wildcard to substitute for characters at the beginning or end of either term or both terms.

flag ***flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **accounting-statistics**—Trace accounting statistics events.
- **all**—Trace all operations.
- **authentication**—Trace authentication events.
- **chap**—Trace CHAP events.
- **events**—Trace interface events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization events.
- **interface-db**—Trace interface database events.
- **lcp**—Trace LCP state machine events.
- **memory**—Trace memory processing events.
- **ncp**—Trace NCP state machine events.
- **packet-error**—Trace packet error events.
- **pap**—Trace PAP events.
- **parse**—Trace parsing events.
- **profile**—Trace libdynamic profile events.
- **receive-packets**—Trace received PPP packets.
- **routing-process**—Trace routing process interactions.
- **rtp**—Trace real-time priority events.
- **rtsock**—Trace routing socket events.
- **session-db**—Trace session database interactions.
- **smi-services-sentry**—Trace SMI services requests and retries.
- **states**—Trace state machine events.
- **transmit-packets**—Trace transmitted PPP packets.
- **tunnel**—Trace L2TP tunneling events.

level—Level of tracing to perform. You can specify any of the following levels:

- **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: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** 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

- Tracing PPP Service Operations for Subscriber Access on page 81

unit (Dynamic PPPoE)

Syntax

```
unit logical-unit-number {
  keepalives interval seconds;
  no-keepalives;
  pppoe-options {
    underlying-interface interface-name;
    server;
  }
  ppp-options {
    authentication [ authentication-protocols ];
    chap {
      challenge-length minimum minimum-length maximum maximum-length;
    }
    pap;
  }
  family inet {
    unnumbered-address interface-name;
    address address;
    service {
      input {
        service-set service-set-name {
          service-filter filter-name;
        }
        post-service-filter filter-name;
      }
      output {
        service-set service-set-name {
          service-filter filter-name;
        }
      }
    }
    filter {
      input filter-name {
        precedence precedence;
      }
      output filter-name {
        precedence precedence;
      }
    }
  }
  filter {
    input filter-name;
    output filter-name;
  }
}
```

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces pp0]

Release Information Statement introduced in Junos OS Release 10.1.

Description In a dynamic profile, configure a logical unit number for the dynamic PPPoE logical interface. You must configure a logical interface to be able to use the router.

Options

logical-unit-number—Variable used to specify the unit number when the PPPoE logical interface is dynamically created. In the **unit *logical-unit-number*** statement for dynamic PPPoE logical interfaces, you must use the predefined variable **$junos-interface-unit** in place of ***logical-unit-number***. The **$junos-interface-unit** predefined variable is dynamically replaced with the unit number supplied by the router when the subscriber logs in.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring a Basic PPPoE Dynamic Profile*
- *Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview*

PART 3

Administration

CHAPTER 6

Verifying and Managing Configurations

Verifying and Managing PPP Configuration for Subscriber Management

Purpose View or clear information about PPP configuration for subscriber management.

Action

- To display information about PPP interfaces:

  user@host> show ppp interface

- To display PPP statistics information:

  user@host> show ppp statistics

- To display PPP session summary information:

  user@host> show ppp summary

- To display PPP address-pool information:

  user@host>show ppp address-pool

Related Documentation

- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 5
- CLI Explorer

CHAPTER 7

Monitoring Commands

- show ppp interface
- show ppp statistics
- show ppp summary
- show ppp address-pool

show ppp interface

Syntax show ppp interface *interface-name*
<extensive| terse>

Release Information Command introduced in Junos OS Release 7.5.

Description Display information about PPP interfaces.

Options ***interface-name***—Name of a logical interface.

extensive | terse—(Optional) Display the specified level of output.

Required Privilege Level view

List of Sample Output
show ppp interface on page 68
show ppp interface extensive on page 68
show ppp interface terse on page 68

Output Fields Table 5 on page 60 lists the output fields for the **show ppp interface** command. Output fields are listed in the approximate order in which they appear.

Table 5: show ppp interface Output Fields

Field Name	Field Description	Level of Output
Session	Name of the logical interface on which the session is running.	All levels
Type	Session type: PPP.	All levels
Phase	PPP process phase: **Authenticate**, **Pending**, **Establish**, **LCP**, **Network**, **Disabled**, and **Tunneled**.	All levels
Session flags	Special conditions present in the session: **Bundled**, **TCC**, **No-keepalives**, **Looped**, **Monitored**, and **NCP-only**.	All levels
***protocol* State**	Protocol state information. See specific protocol state fields for information.	None specified
AUTHENTICATION	Challenge-Handshake Authentication Protocol (CHAP) authentication state information or Password Authentication Protocol (PAP) state information. See the **Authentication** field description for further information.	None specified

Table 5: show ppp interface Output Fields *(continued)*

Field Name	Field Description	Level of Output
Keepalive settings	Keepalive settings for the PPP sessions on the L2TP network server (LNS). LNS based PPP sessions are supported only on service interfaces (si). • **Interval**—Time in seconds between successive keepalive requests. Keepalive aging timeout is calculated as a product of the **interval** and **Down-count** values. If the keepalive aging timeout is greater than 180 seconds, the keepalive packets are handled by the Routing Engine. If the aging timeout is less than or equal to 180 seconds, the packets are handled by the Packet Forwarding Engine. • **Up-count**—The number of keepalive packets a destination must receive to change a link's status from down to up. • **Down-count**—The number of keepalive packets a destination must fail to receive before the network takes down a link.	**extensive**
RE Keepalive statistics	Keepalive statistics for the packets handled by the Routing Engine. • **LCP echo req Tx**—LCP echo requests sent from the Routing Engine. • **LCP echo req Rx**—LCP echo requests received at the Routing Engine. • **LCP echo rep Tx**—LCP echo responses sent from the Routing Engine. • **LCP echo rep Rx**—LCP echo responses received at the Routing Engine. • **LCP echo req timeout**—Number of keepalive packets where the keepalive aging timer has expired. • **LCP Rx echo req Magic Num Failures**—LCP echo requests where the magic numbers shared between the PPP peers during LCP negotiation did not match. • **LCP Rx echo rep Magic Num Failures**—LCP echo responses where the magic numbers shared between the PPP peers during LCP negotiation did not match.	**extensive**

Table 5: show ppp interface Output Fields *(continued)*

Field Name	Field Description	Level of Output

LCP	**LCP information:**
	• **State**—LCP protocol state (all platforms except M120 and M320 routers):
	  • **Ack-rcvd**—A Configure-Request has been sent and a Configure-Ack has been received.
	  • **Ack-sent**—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.
	  • **Closed**—Link is not available for traffic.
	  • **Opened**—Link is administratively available for traffic.
	  • **Req-sent**—An attempt has been made to configure the connection.
	• **State**—LCP protocol state (M120 and M320 routers):
	  • **Ack-rcvd**—A Configure-Request has been sent and a Configure-Ack has been received.
	  • **Ack-sent**—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.
	  • **Closed**—Link is available (up), but no Open has occurred.
	  • **Closing**—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.
	  • **Opened**—Link is administratively available for traffic. A Configure-Ack has been both sent and received.
	  • **Req-sent**—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received.
	  • **Starting**—An administrative Open has been initiated, but the lower layer is still unavailable (Down).
	  • **Stopped**—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack.
	  • **Stopping**—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.
	• **Last started**—LCP state start time.
	• **Last completed**—LCP state completion time.
		extensive

Table 5: show ppp interface Output Fields *(continued)*

Field Name	Field Description	Level of Output

	• **Negotiated options**:
	  • **ACFC**—Address and-Control Field Compression. A configuration option that provides a method to negotiate the compression of the Data Link Layer Address and Control fields.
	  • **Asynchronous map**—Asynchronous control character map. A configuration option used on asynchronous links such as telephone lines to identify control characters that must be replaced by a two-character sequence to prevent them from being interpreted by equipment used to establish the link.
	  • **Authentication protocol**—Protocol used for authentication. This option provides a method to negotiate the use of a specific protocol for authentication. It requires a peer to authenticate itself before allowing network-layer protocol packets to be exchanged. By default, authentication is not required.
	  • **Authentication algorithm**—Type of authentication algorithm. The Message Digest algorithm (MD5) is the only algorithm supported.
	  • **Endpoint discriminator class**—For multilink PPP (MLPPP), a configuration option that identifies the system transmitting the packet. This option advises a system that the peer on this link could be the same as the peer on another existing link.
	  • **Magic number**—A configuration option that provides a method to detect looped-back links and other data-link layer anomalies. By default, the magic number is not negotiated.
	  • **MRU**—Maximum receive unit. A configuration option that may be sent to inform the peer that the implementation can receive larger packets, or to request that the peer send smaller packets. The default value is 1500 octets.
	  • **MRRU**—For multilink PPP, the maximum receive reconstructed unit. A configuration option that specifies the maximum number of octets in the Information fields of reassembled packets.
	  • **Multilink header suspendable classes**—For MLPPP, an LCP option that advises the peer that the implementation wishes to receive fragments with a format given by the code number, with the maximum number of suspendable classes given.
	  • **Multilink header format classes**—For MLPPP, an LCP option that advises the peer that the implementation wishes to receive fragments with a format given by the code number.
	  • **PFC**—Protocol-Field-Compression. A configuration option that provides a method to negotiate the compression of the PPP Protocol field.
	  • **short sequence**—For MLPPP, an option that advises the peer that the implementation wishes to receive fragments with short, 12-bit sequence numbers.	

Table 5: show ppp interface Output Fields *(continued)*

Field Name	Field Description	Level of Output
Authentication	CHAP or PAP authentication state information. For CHAP authentication: • **Chap-ans-rcvd**—Packet was sent from the peer, indicating that the peer received the **Chap-resp-sent** packet. • **Chap-ans-sent**—Packet was sent from the authenticator, indicating that the authenticator received the peer's **Chap-resp-rcvd** packet. • **Chap-chal-rcvd**—Challenge packet has been received by the peer. • **Chap-chal-sent**—Challenge packet has been sent by the authenticator to begin the CHAP protocol or has been transmitted at any time during the Network-Layer Protocol (NCP) phase to ensure that the connection has not been altered. • **Chap-resp-rcvd**—CHAP response packet has been received by the authenticator. • **Chap-resp-sent**—CHAP response packet has been sent to the authenticator. • **Closed**—Link is not available for authentication. • **Failure**—Authenticator compares the response value in the response packet from the peer with its own response value, but the value does not match. Authentication fails. • **Success**—Authenticator compares the response value in the response packet from the peer with its own response value, and the value matches. Authentication is successful. For PAP authentication: • **Pap-resp-sent**—PAP response sent to peer (ACK/NACK)t. • **Pap-req-rcvd**—PAP request packet received from peer. • **Pap-resp-rcvd**—PAP response received from the peer (ACK/NACK). • **Pap-req-sent**—PAP request packet sent to the peer. • **Closed**—Link is not available for authentication. • **Failure**—Authenticator compares the response value in the response packet from the peer with its own response value, but the value does not match. Authentication fails. • **Success**—Authenticator compares the response value in the response packet from the peer with its own response value, and the value matches. Authentication is successful.	None specified

Table 5: show ppp interface Output Fields *(continued)*

Field Name	Field Description	Level of Output

IPCP	Internet Protocol Control Protocol (IPCP) information.
	• **State**—(All platforms except M120 and M320 routers) One of the following values:
	  • **Ack-rcvd**—A Configure-Request has been sent and a Configure-Ack has been received.
	  • **Ack-sent**—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.
	  • **Closed**—Link is not available for traffic.
	  • **Opened**—Link is administratively available for traffic.
	  • **Req-sent**—An attempt has been made to configure the connection.
	• **State**—(M120 and M320 routers) One of the following values:
	  • **Ack-rcvd**—A Configure-Request has been sent and a Configure-Ack has been received.
	  • **Ack-sent**—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.
	  • **Closed**—Link is available (up), but no Open has occurred.
	  • **Closing**—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.
	  • **Opened**—Link is administratively available for traffic. A Configure-Ack has been both sent and received.
	  • **Req-sent**—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received.
	  • **Starting**—An administrative Open has been initiated, but the lower layer is still unavailable (Down).
	  • **Stopped**—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack.
	  • **Stopping**—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.
	• **Last started**—IPCP state start time.
	• **Last completed**—IPCP state authentication completion time.
	• **Negotiated options:**
	  • **compression protocol**—Negotiate the use of a specific compression protocol. By default, compression is not enabled.
	  • **local address**—Desired local address of the sender of a Configure-Request. If all four octets are set to zero, the peer provides the IP address.
	  • **primary DNS server**—Negotiate with the remote peer to select the address of the primary DNS server to be used on the local end of the link.
	  • **primary WINS server**—Negotiate with the remote peer to select the address of the primary WINS server to be used on the local end of the link.
	  • **remote address**—IP address of the remote end of the link in dotted quad notation.
	  • **secondary DNS server**—Negotiate with the remote peer to select the address of the secondary DNS server to be used on the local end of the link.
	  • **secondary WINS server**—Negotiate with the remote peer to select the address of the secondary WINS server to be used on the local end of the link.
	• **Negotiation mode**—PPP Network Control Protocol (NCP) negotiation mode configured for IPCP: **Active** or **Passive**
		extensive

Table 5: show ppp interface Output Fields *(continued)*

Field Name	Field Description	Level of Output

IPV6CP	Internet Protocol version 6 Control Protocol (IPv6CP) information.
	• **State**—(All platforms except M120 and M320 routers) One of the following values:
	  • **Ack-rcvd**—A Configure-Request has been sent and a Configure-Ack has been received.
	  • **Ack-sent**—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.
	  • **Closed**—Link is not available for traffic.
	  • **Opened**—Link is administratively available for traffic.
	  • **Req-sent**—An attempt has been made to configure the connection.
	• **State**—(M120 and M320 routers) One of the following values:
	  • **Ack-rcvd**—A Configure-Request has been sent and a Configure-Ack has been received.
	  • **Ack-sent**—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.
	  • **Closed**—Link is available (up), but no Open has occurred.
	  • **Closing**—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.
	  • **Opened**—Link is administratively available for traffic. A Configure-Ack has been both sent and received.
	  • **Req-sent**—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received.
	  • **Starting**—An administrative Open has been initiated, but the lower layer is still unavailable (Down).
	  • **Stopped**—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack.
	  • **Stopping**—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.
	• **Last started**—IPV6CP state start time.
	• **Last completed**—IPV6CP state authentication completion time.
	• **Negotiated options**:
	  • **local interface identifier**—Desired local address of the sender of a Configure-Request. If all four octets are set to zero, the peer provides the IP address.
	  • **remote interface identifier**—IP address of the remote end of the link in dotted quad notation.
	• **Negotiation mode**—PPP Network Control Protocol (NCP) negotiation mode configured for IPv6CP: **Active** or **Passive**
		extensive

Table 5: show ppp interface Output Fields *(continued)*

Field Name	Field Description	Level of Output

OSINLCP State	OSI Network Layer Control Protocol (OSINLCP) protocol state information (all platforms except M120 and M320 routers):
	• **State:**
	  • **Ack-rcvd**—Configure-Request has been sent and Configure-Ack has been received.
	  • **Ack-sent**—Configure-Request and Configure-Ack have both been sent, but Configure-Ack has not yet been received.
	  • **Closed**—Link is not available for traffic.
	  • **Opened**—Link is administratively available for traffic.
	  • **Req-sent**—Attempt has been made to configure the connection.
	• **Last started**—OSINLCP state start time.
	• **Last completed**—OSINCLP state completion time.
		extensive

TAGCP	TAGCP information.
	• **State**—(All platforms except M120 and M320 routers) One of the following values:
	  • **Ack-rcvd**—A Configure-Request has been sent and a Configure-Ack has been received.
	  • **Ack-sent**—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.
	  • **Closed**—Link is not available for traffic.
	  • **Opened**—Link is administratively available for traffic.
	  • **Req-sent**—An attempt has been made to configure the connection.
	• **State**—(M120 and M320 routers) One of the following values:
	  • **Ack-rcvd**—A Configure-Request has been sent and a Configure-Ack has been received.
	  • **Ack-sent**—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received.
	  • **Closed**—Link is available (up), but no Open has occurred.
	  • **Closing**—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.
	  • **Opened**—Link is administratively available for traffic. A Configure-Ack has been both sent and received.
	  • **Req-sent**—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received.
	  • **Starting**—An administrative Open has been initiated, but the lower layer is still unavailable (Down).
	  • **Stopped**—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack.
	  • **Stopping**—A Terminate-Request has been sent but a Terminate-Ack has not yet been received.
	• **Last started**—TAGCP state start time.
	• **Last completed**—TAGCP state authentication completion time.
		extensive
		none

Sample Output

show ppp interface

```
user@host> show ppp interface si-1/3/0.0
Session si-1/3/0.0, Type: PPP, Phase: Authenticate
  Session flags: Monitored
    LCP State: Opened
    AUTHENTICATION: CHAP State: Chap-resp-sent, Chap-ans-sent
    IPCP State: Closed, OSINLCP State: Closed
```

show ppp interface extensive

```
user@host> show ppp interface si-0/0/3.0 extensive

    Session si-0/0/3.0, Type: PPP, Phase: Network
        Keepalive settings: Interval 30 seconds, Up-count 1, Down-count 3
RE Keepalive statistics:
  LCP echo req Tx        :  657 (last sent 00:50:10 ago)
  LCP echo req Rx        :    0 (last seen: never)
  LCP echo rep Tx        :    0
  LCP echo rep Rx        :  657
  LCP echo req timout    :    0
  LCP Rx echo req Magic Num Failures :    0
  LCP Rx echo rep Magic Num Failures :    0
LCP
  State: Opened
  Last started: 2007-01-29 10:43:50 PST
  Last completed: 2007-01-29 10:43:50 PST
  Negotiated options:
    Authentication protocol: PAP, Magic number: 2341124815, MRU: 4470
Authentication: PAP
  State: Success
  Last started: 2007-01-29 10:43:50 PST
  Last completed: 2007-01-29 10:43:50 PST
IPCP
  State: Opened
  Last started: 2007-01-29 10:43:50 PST
  Last completed: 2007-01-29 10:43:50 PST
  Negotiated options:
    Local address: 10.10.10.1, Remote address: 10.10.10.2
  Negotiation mode: Active
IPV6CP
  State: Opened
  Last started: 2007-01-29 10:43:50 PST
  Last completed: 2007-01-29 10:43:50 PST
  Negotiated options:
    Local interface identifier: 2a0:a522:64:d319, Remote interface identifier: 0:0:0:c
  Negotiation mode: Passive
```

show ppp interface terse

```
user@host> show ppp interface si-1/3/0 terse
Session name    Session type   Session phase      Session flags
si-1/3/0.0      PPP            Authenticate       Monitored
```

show ppp statistics

Syntax show ppp statistics
<detail>
<memory>
<recovery>

Release Information Command introduced in Junos OS Release 7.5.

Description Display PPP interface statistics information.

Options **detail**—(Optional) Display the detailed statistics.

memory—(Optional) Display PPP process memory statistics.

recovery—(Optional) Display recovery state of PPP after a GRES or restart. It is safe to force another GRES or restart only when the recovery state indicates the recovery is done.

NOTE: When you issue this command option during the recovery process, the command may time out or fail silently rather than display output. Recovery is not complete until the command displays **Recovery state: recovery done.**

Required Privilege Level view

List of Sample Output
show ppp statistics on page 73
show ppp statistics detail on page 73
show ppp statistics recovery (Safe to Restart) on page 74
show ppp statistics recovery (Unsafe to Restart) on page 74

Output Fields Table 6 on page 69 lists the output fields for the **show ppp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 6: show ppp statistics Output Fields

Field Name	Field Description	Level of Output
Total sessions	Number of PPP sessions on an interface.	none **detail**
Sessions in disabled phase	Number of PPP sessions disabled. Number of sessions where the link is either administratively or physically down. Once the PPP process learns from the kernel that Layer 2 is ready to send and receive traffic, it will do a phase transition from disabled to established. When LCP and NCP transitions through states, links transition to the establish phase when terminate packets are exchanged or some other failure, such as authentication or expiration of a timer occurs.	none **detail**

Table 6: show ppp statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Sessions in establish phase	Number of PPP sessions in establish phase. In order to establish communications over a point-to-point link, each end of the PPP link must first send LCP packets to configure and test the data link.	none **detail**
Sessions in authenticate phase	Number of PPP sessions in authenticate phase. Each end of the PPP link must first send LCP packets to configure the data link during the link establishment phase. After the link has been established, PPP provides for an optional authentication phase before proceeding to the Network-Layer Protocol (NLP) phase.	none **detail**
Sessions in network phase	Number of PPP sessions in the network phase. After a link has been established and optional facilities have been negotiated as needed by the LCP, PPP must send Network Control Protocol (NCP) packets to choose and configure one or more network-layer protocols, such as IP, IPX, or AppleTalk. Once each of the chosen network-layer protocols has been configured, datagrams from each network-layer protocol can be sent over the link.	none **detail**
Bundles in pending phase	Number of unique bundles to which PPP links are referring.	none **detail**
Type	Type of structure for which memory is allocated. • **Queued rtsock msgs**—Queued route socket messages. When a PPP process is unable to send a route socket message to the kernel (typically because of congestion of the route socket interface), the message is queued for deferred processing. • **PPP session**—Active PPP session. Stores all the information for a PPP session, such as authentication, sequence number, LCP session, and NCP session information. • **Interface address**—Interface address associated with a PPP connection. Stores the information about the interface address that PPP obtains from the kernel. • **Destination profile**—Stores the destination profile information associated with an interface address. • **ML link settings**—Stores information about an MLPPP link, such as the bundle name and compressed real-time transport protocol (CRTP) settings. • **IPCP blocked address**—When addresses are blocked in an address pool (for example, when the interface address is within the range of an address pool, it will be implicitly blocked), this structure is used to store the address in the pool. • **PPP session trace**—A PPP session trace is allocated for record keeping for each session listed at the [**set protocols ppp monitor-session**] hierarchy level. • **IFL redundancy state**—Stores redundancy state information needed for high availability (HA) operation. • **Protocol family**—Stores the information about the protocol family that PPP obtains from the kernel.	**detail**

Table 6: show ppp statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Type (continued)	• **ML bundle settings**—Multilink bundle settings. Stores the context information for a MLPPP bundle. • **PPP LCP session**—PPP Link Control Protocol session, used for establishing, configuring, and testing the data-link connection. Stores the information for an LCP session, such as negotiated options, current state, and statistics. • **PPP NCP session**—PPP Network Control Protocol (NCP) phase in the PPP link connection process. Stores the information for an NCP session, such as negotiated options, current state, address family, and statistics. • **Physical interface**—Stores the information about the physical interface that PPP obtains from the kernel. • **Access profile**—Stores the information found at the [**edit access profile**] hierarchy level for each profile. • **ML wait entry**—Created when there are MLPPP links joining a bundle. before its addition to the PPP process. Links are saved here, and when the bundle is added, are properly assigned to the bundle. • **Group profile**—Stores information set in the PPP stanza of a group profile, such as the primary and secondary Domain Name System (DNS), primary and secondary NDNS, and address pool name. • **Profile client**—Stores the per-client information of the access profile (information obtained from the [**set access profile *name* client *client-name***] hierarchy level. • **PPP Auth session**—PPP authentication session. Stores all the session-specific authentication protocol parameters. • **Logical interface**—Stores the information about the logical interface that PPP obtains from the kernel. • **Non-tagged**—Generic catch-all for allocations not of a particular structure type.	**detail**

Table 6: show ppp statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Type	If you specify the **memory** keyword, the following memory statistics are displayed for Ethernet interfaces on M120 and M320 routers. • **authenticate**—Stores information common to all PPP authentication protocols. • **linkInterface**—Stores information about PPP link interfaces. • **pap**—Stores information about PPP PAP authentication protocol. Includes authenticator and authenticate state machines. • **lcp**—PPP Link Control Protocol session. Used for establishing, configuring and testing the data-link connection. Stores information for LCP session, such as negotiated options, state, and statistics. • **chap**—Stores information about PPP CHAP authentication protocol. Includes authenticator and authenticate state machines. • **eapBuffer**—Stores runtime authentication information for EAP. • **eap**—Stores information about PPP EAP authentication protocol. Includes authenticator and authenticate state machines. • **authNone**—Stores information about no PPP authentication. Includes the authenticator state machine. • **networkInterface**—Stores information about NCP portions of PPP protocol. • **ipNcp**—PPP IPCP session information. Used for configuring, negotiating, and establishing IPCP protocol. Stores the current state, and configured and negotiated options. • **ipv6Ncp**—PPP IPv6CP session information. Used for configuring, negotiating, and establishing IPv6CP protocol. Stores the current state, and configured and negotiated options. • **osiNcp**—PPP OSICP session information. Used for configuring, negotiating, and establishing OSICP protocol. Stores the current state, and configured and negotiated options. • **mplsNcp**—PPP MPLSCP session information. Used for configuring, negotiating, and establishing MPLSCP protocol. Stores the current state. • **trace**—Stores information for PPP debugging.	**memory**
Total	Total memory allocations.	**detail**
Size	Size of the structure.	**detail**
Active	Number of instances of the structure that are used.	**detail**
Free	Number of instances of the structure that are on the free list. Types with a number in the **Free** column are pooled structures, and are typically types that are often used.	**detail**
Limit	Maximum number of instances that can be on the free list. Types with a number in the **Limit** column are pooled structures, and are typically types that are often used.	**detail**
Total size	Total amount of memory being used by a type of structure (includes active and free instances).	**detail**
Requests	Number of allocation requests made by a type of structure.	**detail**

Table 6: show ppp statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Failures	Number of failed allocations.	**detail**
Recovery state	State of PPP recovery after a GRES or restart: • recovery done—All sessions have recovered; it is safe to force another GRES or restart. • recovery cleanup pending—Not all PPP sessions have recovered; it is not safe to force another GRES or restart.	none
Subscriber sessions pending retention	Number of PPP subscriber sessions that are in the process of being recovered.	none
Subscriber sessions recovered OK	Number of PPP subscriber sessions that have recovered after a GRES or restart.	none
Subscriber sessions recovery failed	Number of PPP subscriber sessions that have failed to recover after a GRES or restart.	none

Sample Output

show ppp statistics

```
user@host> show ppp statistics
Session statistics from PPP process
  Total sessions: 0
    Sessions in disabled phase    : 0
    Sessions in establish phase   : 0
    Sessions in authenticate phase: 0
    Sessions in network phase     : 0
    Bundles in pending phase      : 0

Session statistics from PPP universal edge process
  Total subscriber sessions: 32
    Subscriber sessions in disabled phase    : 32
    Subscriber sessions in establish phase   : 0
    Subscriber sessions in authenticate phase: 0
    Subscriber sessions in network phase     : 0
```

show ppp statistics detail

```
user@host> show ppp statistics detail
Session statistics from PPP process
  Total sessions: 0
    Sessions in disabled phase    : 0
    Sessions in establish phase   : 0
    Sessions in authenticate phase: 0
    Sessions in network phase     : 0
    Bundles in pending phase      : 0
Type                  Size  Active  Free  Limit  Total size  Requests Failures
Queued rtsock msgs      28       0     0  65535           0         0
PPP session             60       0                       0         0
Interface address       64       0     0  65535           0         0
Destination profile     65       0                       0         0
ML link settings        68       0                       0         0
```

```
IPCP blocked address      68      0                      0         0
PPP session trace         76      0                      0         0
IFL redundancy state      76      0                      0         0
Protocol family           84      0      0  65535        0         0
ML bundle settings       108      0                      0         0
PPP LCP session          120      0                      0         0
PPP NCP session          124      0                      0         0
Physical interface       124    170      0  65535    21080       170
Access profile           132      0                      0         0
ML wait entry            144      0      0     20        0         0
Group profile            164      0                      0         0
Profile client           272      0                      0         0
PPP Auth session         356      0                      0         0
Logical interface        524      0      0  65535        0         0
Non-tagged                                              8         2
Total                                                21088       172       0

Session statistics from PPP universal edge process
  Total subscriber sessions: 32
    Subscriber sessions in disabled phase    : 32
    Subscriber sessions in establish phase   : 0
    Subscriber sessions in authenticate phase: 0
    Subscriber sessions in network phase     : 0
Type                   Size  Active  Free  Limit  Total size Requests Failures
authenticate            224       1    99  16384         224        0        0
linkInterface           152       1    99  16384         152        0        0
pap                     256       1    99  16384         256        0        0
lcp                     272       1    99  16384         272        0        0
chap                    284       0     0  16384           0        0        0
eapBuffer              1464       0     0  16384           0        0        0
eap                     276       0     0  16384           0        0        0
authNone
networkInterface        220       1    99  16384         220        0        0
ipNcp                   256       1    99  16384         256        0        0
ipv6Ncp                 204       0     0  16384           0        0        0
osiNcp                  192       0     0  16384           0        0        0
mplsNcp                 188       0     0  16384           0        0        0
trace                  2052       0    16     16           0        0        0
Total                                                   1380        0        0
```

show ppp statistics recovery (Safe to Restart)

```
user@host> show ppp statistics recovery
Recovery statistics from PPP universal edge process
  Recovery state: recovery done
    Subscriber sessions recovered OK      : 32001
    Subscriber sessions recovery failed   : 0
```

show ppp statistics recovery (Unsafe to Restart)

```
user@host> show ppp statistics recovery
Recovery statistics from PPP universal edge process
  Recovery state: recovery cleanup pending
    Subscriber sessions pending retention : 32001
    Subscriber sessions recovered OK      : 0
    Subscriber sessions recovery failed   : 0
```

show ppp summary

Syntax show ppp summary

Release Information Command introduced in Junos OS Release 7.5.

Description Display PPP session summary information.

Options This command has no options.

Required Privilege Level view

List of Sample Output show ppp summary on page 75

Output Fields Table 7 on page 75 lists the output fields for the **show ppp summary** command. Output fields are listed in the approximate order in which they appear.

Table 7: show ppp summary Output Fields

Field Name	Field Description
Interface	Interface on which the PPP session is running. An interface type of pp0 indicates an Ethernet interface type on a M120 or M320 router.
Session type	Type of session: **PPP** or **Cisco-HDLC**.
Session phase	PPP process phases: **Authenticate**, **Pending**, **Establish**, **Network**, **Disabled**.
Session flags	Special conditions present in the session, such as **Bundled**, **TCC**, **No-keepalives**, **Looped**, **Monitored**, and **NCP-only**.

Sample Output

show ppp summary

```
user@host> show ppp summary
Interface       Session type  Session phase      Session flags
at-4/0/0.456    PPP           Network
lsq-0/3/0.0     PPP           Disabled
lsq-1/0/0.0     PPP           Disabled
rlsq0.0         PPP           Network            NCP-only
so-1/0/0.0      PPP           Authenticate
so-1/0/1.0      PPP           Disabled           Looped
so-2/0/0.0      Cisco-HDLC    Establish
so-4/0/0.0      PPP           Establish          Monitored
t1-1/3/0:1.0    PPP           Network            Bundled
t1-1/3/0:2.0    PPP           Network            Bundled
pp0.12          PPP           Network
```

show ppp address-pool

Syntax show ppp address-pool *pool-name*
<detail>

Release Information Command introduced in Junos OS Release 7.5.

Description Display PPP address pool information.

Options ***pool-name***—Address pool name.

detail—(Optional) Display detailed address pool information.

Required Privilege Level view

Related Documentation
- Verifying and Managing PPP Configuration for Subscriber Management on page 57

List of Sample Output
show ppp address-pool on page 77
show ppp address-pool detail on page 77

Output Fields Table 8 on page 76 lists the output fields for the **show ppp address-pool** command. Output fields are listed in the approximate order in which they appear.

Table 8: show ppp address-pool Output Fields

Field Name	Field Description	Level of Output
Address pool	Trace address pool code.	All levels
Address range	Range of sequentially ordered IP addresses contained in the address pool.	**detail**
Number of assigned addresses	Fixed IP address that is to be given to remote users when they dial in. This is a host-only IP address (subnet mask is 255.255.255.255) and is only for single connection receiver profiles.	All levels
Number of addresses configured	Number of IP addresses that are available for allocation and used by PPP sessions.	All levels
Assigned addresses	Addresses assigned to PPP sessions from the address pool.	**detail**

Sample Output

show ppp address-pool

```
user@host> show ppp address-pool
Address pool ppp1
  Address range: 10.10.220.1 - 10.10.220.10
  Number of assigned addresses: 0
  Number of addresses configured: 10
```

show ppp address-pool detail

```
user@host> show ppp address-pool ppp1 detail
Address pool ppp1
  Address range: 10.10.220.1 - 10.10.220.10
  Number of assigned addresses: 2
  Number of addresses configured: 10
  Assigned addresses:
      10.10.220.1
      10.10.220.2
```

PART 4

Troubleshooting

CHAPTER 8

Acquiring Troubleshooting Information

Tracing PPP Service Operations for Subscriber Access

The Junos OS trace feature tracks PPP service 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 **jpppd**. 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 PPP service tracing operations:

1. (Optional) Configure a trace log filename.

   See "Configuring the PPP Service Trace Log Filename" on page 82.

2. (Optional) Configure the number and size of trace logs.

   See "Configuring the Number and Size of PPP Service Log Files" on page 82.

3. (Optional) Configure user access to trace logs.

   See "Configuring Access to the PPP Service Log File" on page 83.

4. (Optional) Configure a regular expression to filter the information to be included in the trace log.

   See "Configuring a Regular Expression for PPP Service Messages to Be Logged" on page 83.

5. (Optional) Configure flags to specify which events are logged.

   See "Configuring the PPP Service Tracing Flags" on page 84.

6. (Optional) Configure a severity level for messages to specify which event messages are logged.

   See "Configuring the Severity Level to Filter Which PPP Service Messages Are Logged" on page 85.

Configuring the PPP Service Trace Log Filename

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

To configure the filename for PPP service tracing operations:

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

```
[edit protocols ppp-service traceoptions]
user@host# set file ppp-service_logfile_1
```

Related Documentation

- Tracing PPP Service Operations for Subscriber Access on page 81

Configuring the Number and Size of PPP Service 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 ppp-service traceoptions]
  user@host# set file ppp-service_1 _logfile_1 files 20 size 2097152
  ```

Related Documentation

- Tracing PPP Service Operations for Subscriber Access on page 81

Configuring Access to the PPP Service 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 ppp-service traceoptions]
  user@host# set file ppp-service_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 ppp-service traceoptions]
  user@host# set file ppp-service_1 _logfile_1 no-world-readable
  ```

Related Documentation

- Tracing PPP Service Operations for Subscriber Access on page 81

Configuring a Regular Expression for PPP Service Messages to Be Logged

By default, the trace operation output includes all lines 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 ppp-service traceoptions]
  user@host# set file ppp-service_1 _logfile_1 match regex
  ```

Related Documentation

- Tracing PPP Service Operations for Subscriber Access on page 81

Configuring the PPP Service 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 ppp-service traceoptions]
  user@host# set flag flag
  ```

Related Documentation

- Tracing PPP Service Operations for Subscriber Access on page 81

Configuring Subscriber Filtering for PPP Service Trace Operations

You can apply filters to the PPP service to limit tracing to particular subscribers or domains. Subscriber filtering simplifies troubleshooting in a scaled environment by enabling you to focus on a reduced set of trace results.

For subscriber usernames that have the expected form of ***user*@*domain***, you can filter on the user, the domain, or both. You can use an asterisk (*) as a wildcard to substitute for characters at the beginning or end of either term or both terms to match a greater number of subscribers.

NOTE: **You cannot filter results using a wildcard in the middle of the user or domain terms. For example, the following uses of the wildcard are not supported: tom*25@example.com, tom125@ex*.com.**

When you enable filtering by username, traces that have insufficient information to determine the username are automatically excluded.

To configure subscriber filtering:

- Specify the filter.

  ```
  [edit protocols ppp-service traceoptions]
  user@host# set filter user user@domain
  ```

Consider the following examples of using the wildcard for filtering:

- Filter results for the specific subscriber with the username, tom@example.com.

  ```
  [edit protocols ppp-service traceoptions]
  user@host# set filter user tom@example.com
  ```

- Filter results for all subscribers whose username begins with tom.

  ```
  [edit protocols ppp-service traceoptions]
  user@host# set filter user tom*
  ```

- Filter results for all subscribers whose username ends with tom.

  ```
  [edit protocols ppp-service traceoptions]
  user@host# set filter user *tom
  ```

- Filter results for subscribers with the username tom at all domains beginning with ex.

  ```
  [edit protocols ppp-service traceoptions]
  user@host# set filter user tom@ex*
  ```

- Filter results for all subscribers at all domains that end with ample.com.

  ```
  [edit protocols ppp-service traceoptions]
  user@host# set filter user *ample.com
  ```

- Filter results for all subscribers whose username begins with tom at domains that end with example.com.

  ```
  [edit protocols ppp-service traceoptions]
  user@host# set filter user tom*@*example.com
  ```

Related Documentation

- Tracing PPP Service Operations for Subscriber Access on page 81

Configuring the Severity Level to Filter Which PPP Service 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. A low severity level is less restrictive—filters out fewer messages—than a higher level. When you configure a severity level, all messages at that level and all higher (more restrictive) levels are logged.

The following list presents severity levels in order from lowest (least restrictive) to highest (most restrictive). This order also represents the significance of the messages; for example, **error** messages are of greater concern than **info** messages.

- **verbose**
- **info**
- **notice**
- **warning**
- **error**

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**. You can also specify **verbose** with the same result, because **verbose** is the lowest (least restrictive) severity level; it has nothing to do with the terseness or verbosity of the messages. 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 ppp-service traceoptions]
  user@host# **set level *severity***

Related Documentation

- Tracing PPP Service Operations for Subscriber Access on page 81

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 (Protocols PPP Service)

Syntax

```
traceoptions {
  file <filename> <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  filter {
    aci regular-expression;
    ari regular-expresion;
    service-name regular-expresion;
    underlying-interface interface-name;
    user user@domain;
  }
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level [edit protocols ppp-service]

Release Information Statement introduced in Junos OS Release 9.5.
Option **user** introduced in Junos OS Release 14.1.

Description Define tracing operations for PPP service processes.

Options

file *filename*—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**.

files *number*—(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.

Range: 2 through 1000

Default: 3 files

disable—Disable this trace flag.

filter—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifiers simplifies troubleshooting in a scaled environment.

BEST PRACTICE: Due to the complexity of agent circuit identifiers and agent remote identifiers, we recommend that you do not try an exact match when filtering on these options. For service names, searching on the exact name is appropriate, but you can also use a regular expression with that option.

- **aci** *regular-expression*—Regular expression to match the agent circuit identifier provided by PPP client.
- **ari** *regular-expression*—Regular expression to match the agent remote identifier provided by PPP client.

- **service** ***regular-expression***—Regular expression to match the name of PPPoE service.
- **underlying-interface** ***interface-name***—Name of a PPP underlying interface. You cannot use a regular expression for this filter option.
- **user** *user@domain*—Username of a subscriber. Optionally use an asterisk (*) as a wildcard to substitute for characters at the beginning or end of either term or both terms.

flag ***flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **accounting-statistics**—Trace accounting statistics events.
- **all**—Trace all operations.
- **authentication**—Trace authentication events.
- **chap**—Trace CHAP events.
- **events**—Trace interface events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization events.
- **interface-db**—Trace interface database events.
- **lcp**—Trace LCP state machine events.
- **memory**—Trace memory processing events.
- **ncp**—Trace NCP state machine events.
- **packet-error**—Trace packet error events.
- **pap**—Trace PAP events.
- **parse**—Trace parsing events.
- **profile**—Trace libdynamic profile events.
- **receive-packets**—Trace received PPP packets.
- **routing-process**—Trace routing process interactions.
- **rtp**—Trace real-time priority events.
- **rtsock**—Trace routing socket events.
- **session-db**—Trace session database interactions.
- **smi-services-sentry**—Trace SMI services requests and retries.
- **states**—Trace state machine events.
- **transmit-packets**—Trace transmitted PPP packets.
- **tunnel**—Trace L2TP tunneling events.

level—Level of tracing to perform. You can specify any of the following levels:

- **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: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** 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

- Tracing PPP Service Operations for Subscriber Access on page 81

PART 5

Index

Index

Symbols

A

B

C

D

F

I

K

S

T

U