MX Series Routers as a Service Node in an SRC-Managed Network

Modified: 2015-06-23

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

MX Series Routers as a Service Node in an SRC-Managed Network

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation ix
Documentation and Release Notes ix
Supported Platforms ix
Documentation Conventions ix
Documentation Conventions x
Documentation Feedback xii
Requesting Technical Support xii
Self-Help Online Tools and Resources xiii
Opening a Case with JTAC xiii

Part 1 Overview

Chapter 1 **Software Features Overview 3**

SRC Component Overview 3

Chapter 2 **Service Nodes in an SRC Environment 7**

Service Nodes in an SRC Environment Overview 7
SRC Software in the Service Node Environment 8
Service Node Scenario When the Access Device is Managed by the SRC Software 9
User Login 10
User Logout 11
Using the SRC Software to Support PTSP 11
Accessing the Network Before the SRC Cluster Is Notified About a PTSP Session 11
Accessing the Network After the SRC Cluster Is Notified About a PTSP Session 12
Changing the Network Connection 13
Disconnecting from the Network 14
Terminating the PTSP Session 14

Part 2 Configuration

Chapter 3 **Configuration Tasks for Managing Service Nodes 17**

Configuring SRC Software to Support Service Nodes 17

Part 3 Index

Index 21

List of Figures

Part 1 Overview

Chapter 2 Service Nodes in an SRC Environment 7

Figure 1: SRC Software in the Service Node Environment 8
Figure 2: SRC-Managed Access Nodes in a Service Node Deployment 10

List of Tables

About the Documentation ix
Table 1: Notice Icons x
Table 2: Notice Icons xi
Table 3: Text Conventions xi

Part 1 Overview

Chapter 1 Software Features Overview 3
Table 4: Descriptions of SRC Components 3

About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xii
- Requesting Technical Support on page xii

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:

- C Series

Documentation Conventions

Table 1 on page x 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.

Documentation Conventions

Table 1 on page x defines the notice icons used in this guide. Table 3 on page xi defines text conventions used throughout this documentation.

Table 2: 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 3: Text Conventions

Convention	Description	Examples
Bold text like this	• Represents keywords, scripts, and tools in text. • Represents a GUI element that the user selects, clicks, checks, or clears.	• Specify the keyword **exp-msg**. • Run the **install.sh** script. • Use the **pkgadd** tool. • To cancel the configuration, click **Cancel**.
Bold text like this	Represents text that the user must type.	**user@host# set cache-entry-age** *cache-entry-age*

`Fixed-width text like this`	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	`nic-locators {`
		`  login {`
		`  resolution {`
		`  resolver-name /realms/`
		`  login/A1;`
		`  key-type LoginName;`
		`  value-type SaeId;`
		`  }`

Regular sans serif typeface	• Represents configuration statements. • Indicates SRC CLI commands and options in text. • Represents examples in procedures. • Represents URLs.	• **system ldap server{ stand-alone;** • Use the **request sae modify device failover** command with the **force** option • **user@host# . . .** • http://www.juniper.net/techpubs/software/management/sdx/api-index.html

Table 3: Text Conventions *(continued)*

Italic sans serif typeface	Represents variables in SRC CLI commands.	**user@host# set local-address *local-address***
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <gfwif>.
Key name	Indicates the name of a key on the keyboard.	Press Enter.
Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Italic typeface	• Emphasizes words. • Identifies book names. • Identifies distinguished names. • Identifies files, directories, and paths in text but not in command examples.	• There are two levels of access: *user* and *privileged*. • *SRC-PE Getting Started Guide.* • *o=Users, o=UMC* • The */etc/default.properties* file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class=\ net.juniper.smgt.sae.plugin\ RadiusTrackingPluginEvent
Words separated by the | symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic | line

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/cgi-bin/docbugreport/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software 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 Partner Support Service 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

- Software Features Overview on page 3
- Service Nodes in an SRC Environment on page 7

CHAPTER 1

Software Features Overview

- SRC Component Overview on page 3

SRC Component Overview

The SRC software is a dynamic system. It contains many components that you use to build a subscriber management environment. You can use these tools to customize and extend the SRC software for your use and to integrate the SRC software with other systems. The SRC software also provides the operating system and management tools for C Series Controllers.

Table 4 on page 3 gives a brief description of the components that make up the SRC software.

Table 4: Descriptions of SRC Components

Component	Description
Server Components	
Service activation engine (SAE)	• Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories. • Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases. • Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage.
Subscriber Information Collector (SIC)	Used in conjunction with the MX Series router running the packet-triggered subscribers and policy control (PTSP) solution, the SIC listens for RADIUS accounting events from IP edge devices (accounting clients) and stores them in the Session State Registrar (SSR), or forwards them to a remote AAA server, allowing the SRC software to gain increased subscriber awareness. Additionally, the SIC can optionally edit accounting events before routing them.
Juniper Policy Server (JPS)	Acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and CMTS devices in a PCMM environment.
Network information collector (NIC)	Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
Redirect Server	Redirects HTTP requests received from IP Filter to a captive portal page.
3GPP Gateway	The SRC Third-Generation Partnership Project (3GPP) gateway is a Diameter-based component in the SRC software, which provides integration with 3GPP Policy and Charging Control environments, to provide fixed-mobile convergence (FMC). The SRC 3GPP gateway provides Gx-based integration with the Policy and Charging Rules Function (PCRF). The SRC 3GPP gateway uses the northbound Gx interface to mediate between the PCRF and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The northbound Gx interface on the SRC 3GPP gateway communicates with the PCRF using the Diameter protocol.
3GPP Gy	The SRC 3GPP Gy is a Diameter-based component in the SRC software, which provides Gy-based integration with the Online Charging System (OCS), to provide FMC. The SRC 3GPP Gy uses the northbound Gy interface to handle charging-related information between the OCS and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The northbound Gy interface communicates with the OCS using the Diameter protocol.
Web Application Service	The SRC software includes a Web application server that hosts the Web Services Gateway and the Volume Tracking Application (SRC VTA). In production environments, this application server is designed to host only these applications. However, you can load your own applications into this server for testing or demonstration purposes.
Web Services Gateway	Allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a Simple Object Access Protocol (SOAP) interface. The Web Services Gateway provides the Dynamic Service Activator which allows a gateway client to dynamically activate and deactivate SRC services for subscribers and to run scripts that manage the SAE.
Repository	
Directory	The SRC software includes the Juniper Networks database, which is a built-in Lightweight Directory Access Protocol (LDAP) directory for storing all SRC data including services, policies, and small subscriber databases. For large subscriber databases, you must supply your own directory.
Session State Registrar (SSR)	The SSR is a stateless, highly reliable and highly available database cluster. When used in conjunction with an MX Series router running the packet-triggered subscribers and policy control (PTSP) solution, the SSR stores the IP edge attachment subscriber sessions data learned from IP edge devices in the centralized SSR database.
SRC Configuration and Management Tools	
SRC command line interface (CLI)	Provides a way to configure the SRC software on a C Series Controller from a Junos OS–like CLI. The SRC CLI includes the policies, services, and subscribers CLI, which has separate access privileges.
C-Web interface	Provides a way to configure, monitor, and manage the SRC software on a C Series Controller through a Web browser. The C-Web interface includes a policies, services, and subscribers component, which has separate access privileges.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
Simple Network Management Protocol (SNMP) agent	Monitors system performance and availability. It runs on all the SRC hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps.
Service Management Applications (Run on external system)	
IMS Services Gateway	Integrates into an IP multimedia system (IMS) environment. The SRC software provides a Diameter protocol-based interface that allows the SRC software to integrate with services found on the application layer of IMS.
SRC Programming Interfaces	
NETCONF API	Allows you to configure or request information from the NETCONF server on a C Series Controller that runs the SRC software. Applications developed with the NETCONF API run on a system other than a C Series Controller.
CORBA plug-in service provider interface (SPI)	Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SRC software so that the OSS can be notified of events in the life cycle of SAE sessions. Hosted plug-ins only.
CORBA remote API	Provides remote access to the SAE core API. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
NIC access API	Performs NIC resolutions. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
SAE core API	Controls the behavior of the SRC software. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
Script services	Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network.
VTA API	The Volume Tracking Application (VTA) API is a Simple Object Access Protocol (SOAP) interface that allows developers to create gateway clients and that administrators use to manage VTA subscribers and sessions. The SRC Web Services Gateway allows a gateway client—an application that is not part of the SRC network—to interact with SRC components, such as the VTA, through a SOAP interface.
Authorization and Accounting Applications	
AAA RADIUS servers	Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions. RADIUS servers run on a system other than a C Series Controller.
SRC Admission Control Plug-In (SRC ACP)	Authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages.
Flat file accounting	Stores tracking data to accounting flat files that can be made available to external systems that send the data to a rating and billing system.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
Volume Tracking Application	The SRC Volume Tracking Application (SRC VTA) is an SRC component that allows service providers to track and control the network usage of subscribers and services. You can control volume and time usage on a per-subscriber or per-service basis. This level of control means that service providers can offer tiered services that use volume as a metric, while also controlling abusive subscribers and applications. When a subscriber or service exceeds bandwidth limits (or quotas), the SRC VTA can take actions including imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.
Demonstration Applications (available on the Juniper Networks Website)	
Enterprise Audit Plug-In	Defines a callback interface, which receives events when IT managers complete specified operations.
Enterprise Manager Portal	Allows service providers to provision services for enterprise subscribers on routers running JunosE or Junos OS and allows IT managers to manage services. Enterprise Manager Portal can be used with NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on routers running Junos OS and to all IT managers to make requests about public IP addresses through the Enterprise Manager Portal.
Monitoring Agent application	Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SRC-managed network so that the SAE is notified about subscriber events. The Monitoring Agent application runs on a Solaris platform.
Residential service selection portals	Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment. The Residential service selection portals run on a Solaris platform.
Sample enterprise service portal	Lets service providers supply an interface to their business customers for managing and provisioning services.

Related Documentation

- *SRC Product Description*

CHAPTER 2

Service Nodes in an SRC Environment

- Service Nodes in an SRC Environment Overview on page 7
- Using the SRC Software to Support PTSP on page 11

Service Nodes in an SRC Environment Overview

The Juniper Networks MX Series Ethernet Services Router supports the packet-triggered subscribers and policy control (PTSP) feature that allows the dynamic application of policies on a per-subscriber basis to individual source IP addresses flowing through a given interface. A subscriber context is created for each distinct source IP address seen in a given underlying interface. This feature can be used to support subscribers who are controlled by a subscriber termination device, such as a Broadband Remote Access Service (B-RAS) or gateway GSN (GGSN) device, that is connected to an MX Series router. MX Series routers that support PTSP are called service nodes.

Service nodes act as intelligent policy enforcement points for IP edge devices with these features:

- Single access–agnostic policy enforcement point that allows the easy introduction of new services independent of access technologies. Subscribers and policies are tracked by a subscriber's IP address and do not require subscriber interfaces.
- Single point for management, reporting, and troubleshooting, which includes support for dynamic policy attachment and updates.

When the MX Series router acts as a service node in the SRC environment, the SRC software supports this role by providing subscriber awareness to the service node.

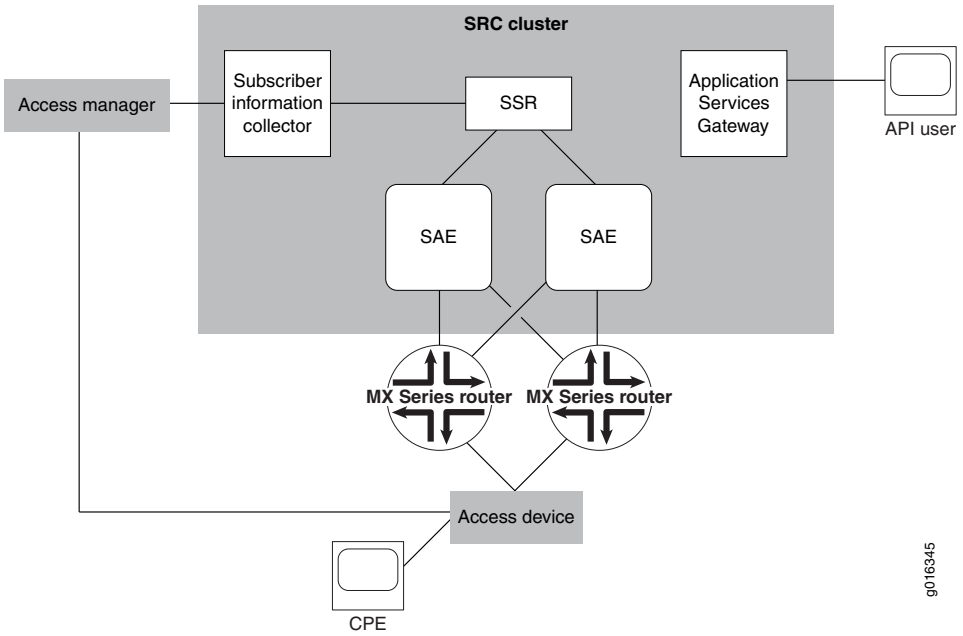
To support service nodes, the SRC software:

- Collects and dispatches RADIUS accounting events.
- Creates an IP edge attachment session and stores it.
- Manages profile and policies for IP address sessions (PTSP sessions) by associating the session with the correct attachment session and sending profile and policy information to the MX Series router.
- Sends start, interim, and stop accounting records containing usage information from the service node and attachment information from the IP edge device.

SRC Software in the Service Node Environment

Figure 1 on page 8 illustrates a simple deployment scenario.

Figure 1: SRC Software in the Service Node Environment



This simple deployment scenario includes the following components:

- Customer premises equipment (CPE)—Equipment with which the network user connects to an IP network. This device can be any device that allows a subscriber to connect to the network—including a wireless phone, a DSL router, or a cable modem.
- Access device—Device that terminates the IP session for the network user. This device must authenticate the network user and notify the access manager when an attachment session is created and stopped. Optionally, the device can notify the access manager when the attachment session is modified. This device can be a gateway GSN (GGSN), a Broadband Remote Access Server (B-RAS), or a cable modem termination system (CMTS).
- Access manager—Device that manages access devices. This device must be able to forward session start/stop notifications to the SRC cluster. This device can be a RADIUS accounting server.
- SRC cluster—Collection of SRC components that manage attachment sessions and PTSP device sessions, including:
  - Subscriber information collector (SIC)—SRC component that receives session start, modification, and stop notifications from the access manager. The start, modification, and stop notifications are RADIUS accounting start, interim update, and stop events.
  - Session State Registrar (SSR)—SRC component that stores attachment sessions and notifies other components about updates.

    - SAE—SRC component that manages service sessions and policies for IP subscriber sessions.
    - Application Services Gateway (ASG), API client—SRC cluster uses the gateway to allow external API clients to manipulate sessions maintained in the cluster.
- MX Series router—MX Series Ethernet Services Router that supports the PTSP feature (service node), which detects IP flows and manages policies for those sessions.

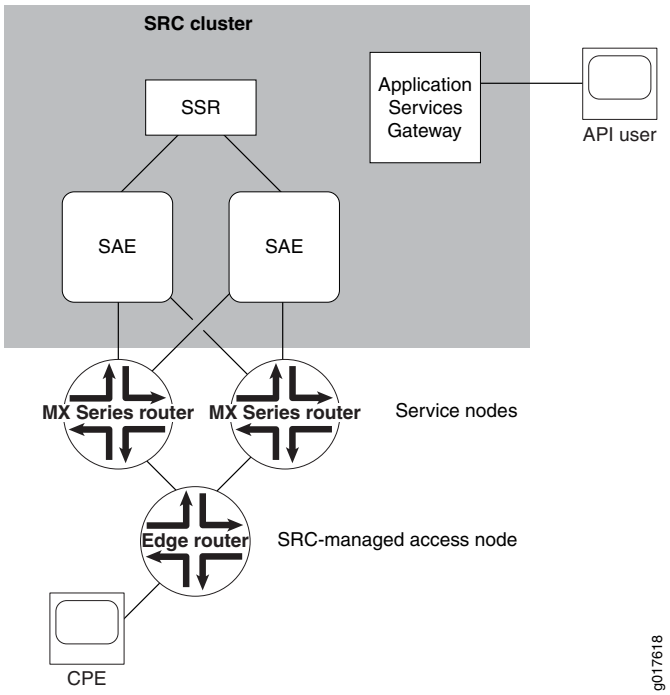
In this simple deployment scenario, the following actions might occur:

1. The CPE connects to an access device, which terminates an IP address and provides lifecycle notifications but provides limited policy management capabilities. The SRC cluster learns about CPE attachment sessions from the access manager.
2. Traffic from the CPE to the network is routed through the MX Series routers that support PTSP (service nodes).
3. The service node detects IP flows from the CPE and notifies the SRC cluster about the IP flow. Traffic from a single CPE can be routed through multiple MX Series routers; each router detects and manages individual flows that must be coordinated on the SRC cluster level.
4. The SRC cluster associates the IP flow information with identity information that it has learned for the CPE attachment session and uses this information to select the appropriate policies for handling the subscriber traffic.

Service Node Scenario When the Access Device is Managed by the SRC Software

In a PTSP deployment scenario where the SRC manages the edge access device, sessions initiated on the access device are written directly to the SSR database—for example, when the PTSP scenario uses a Juniper Networks E Series Broadband Services Router or MX Series Ethernet Services Router (JSRC) as the access device. Figure 2 on page 10 illustrates this deployment scenario.

Figure 2: SRC-Managed Access Nodes in a Service Node Deployment



An SAE user-tracking plug-in publishes subscriber session information to the SSR after the subscriber has successfully logged in through the access node. The SSR writer plug-in is a user-tracking plug-in that creates a user session record and writes it into the SSR. The SSR writer plug-in specifies which SAE plug-in attributes are written to the SSR and the SSR maps the SAE plug-in attributes to SSR attributes. The SSR writer plug-in configuration specifies the association between the SAE plug-in attributes, which are used in the SAE access session and carried in the user-tracking event, and the respective SAE plug-in attributes configured in the SSR association. Plug-in attributes associated with the SSR can be mapped either to the plug-in attributes used to identify the access session or to literal values.

User Login

An access subscriber session can be created before or after the PTSP IP flow is detected.

User Login Scenario When the Access Session is Created Before the PTSP Session

When a user logs in through the SRC-managed access device, a user session is created in the SAE. A user-tracking event is then sent to the SSR writer plug-in, which provides sufficient information to successfully identify the user and store the associated record in the SSR. When the PTSP flow is detected by the SAE, a temporary user session is created and a user authentication event is sent to the SSR reader authentication plug-in to authenticate the user. The SSR reader authentication plug-in reads the record and updates the event with the session attributes read from the SSR. When the user is authenticated, a permanent user session is created and the SAE installs the policies on the service node managing PTSP traffic.

User Login Scenario When the PTSP Session is Created Before the Access Session

The service node detects the new IP flow and creates a PTSP session. The SRC software starts an anonymous subscriber session and the SAE installs policies on the service node. The user logs in through the access device, an access user session is created in the SAE, and the user-tracking event is sent to the SSR writer. The record associated with the subscriber session is stored in the SSR. When the access session is created in the SSR, the identity of the PTSP subscriber session is changed through an SSR event. The SAE receives a notification that contains the IP-Address and VPN-ID attributes. The event handler searches for matching sessions that have been authorized by the SSR reader authentication plug-in and performs a re-authentication of those sessions. If the re-authentication does not change the existing session, the event handler re-evaluates all policies and sends updates to the PTSP router.

User Logout

When the access session is dropped because the user logs out, the SSR writer plug-in updates the session state associated with the user. After the access session state becomes inactive in the SSR, the SAE receives a notification and terminates the PTSP subscriber session associated with the attachment session and all services are deactivated. In the case when the PTSP session is dropped but the access session remains active, the user may activate PTSP services at a later time reusing the same access session stored in the SSR. PTSP session termination does not affect the attachment session.

Related Documentation

- *Subscriber Information Collector Overview*
- *Session State Registrar Overview*
- *Managing Subscriber-Level Policies on MX Series Routers Overview*

Using the SRC Software to Support PTSP

When you use the SRC software to support PTSP on MX Series routers, the SRC software can become aware of the subscribers before or after a PTSP session has been created. This topic describes the interaction among the components in the basic scenario and the sequence of events for different situations.

Accessing the Network Before the SRC Cluster Is Notified About a PTSP Session

The CPE connects to the network and the SRC cluster is notified about the connection before a PTSP session is created. In this case, the attachment session exists before the PTSP session. The sequence of events is:

1. The CPE connects to the network through the access device.
2. The access device notifies the access manager about the session start.
3. The access manager forwards the session start notification to the SIC, which translates the attributes into SRC-specific attributes.
4. The SIC creates an attachment session in the SSR.

5. (Optional) The subscriber activates a service through the ASG. (In the sequence of events, this step is the earliest one for using the ASG.)
6. (Optional) The ASG creates a service session in the SSR that is associated with the attachment session. If the attachment session does not exist, the service activation fails.
7. The CPE accesses the network. The service node detects a new IP flow and creates a PTSP session.
8. The service node notifies the SAE that is currently managing the MX Series router. The SAE extracts the IP address, and optionally the VPN ID, from the PTSP session information.
9. The SAE starts managing the PTSP session and calls the SSR reader authentication plug-in to obtain attachment session information from the SSR. The data from the SSR is used in the classification context.
10. The SAE runs the subscriber classification script, loads a subscriber profile, and creates a subscriber session. The subscriber session activates any subscribed activate-on-login service.
11. When the subscriber session is completely activated, the SAE installs any active policies on the service node.

Accessing the Network After the SRC Cluster Is Notified About a PTSP Session

The CPE connects to the network and the SRC cluster is notified about the connection after a PTSP session is processed. In this case, the attachment session does not exist before the PTSP session. The sequence of events is:

1. The CPE connects to the network through the access device.
2. The CPE accesses the network. The service node detects the new IP flow and creates a PTSP session.
3. The service node notifies the SAE that is currently managing the MX Series router. The SAE extracts the VPN ID from the PTSP session information.
4. The SAE starts managing the PTSP session and calls the SSR reader authentication plug-in to obtain attachment session information from the SSR. No information is returned to the SAE because the attachment session does not exist yet.
5. The SAE creates an unauthenticated (anonymous) subscriber session.
6. When the subscriber session is completely activated, the SAE installs any active policies on the service node.
7. The access device notifies the access manager about the session start.
8. The access manager forwards the session start notification to the SIC.
9. The SIC creates the attachment session in the SSR.
10. The SSR notifies the SAE that the attachment session has been modified. The SAE finds any affected subscriber sessions. The SSR notifies all active SAEs in the same cluster.

11. For any affected subscriber session, the SAE updates the classification context and initiates a login. This login runs the subscriber classification script and compares the result.
    - If the subscriber profile has changed, the existing session is terminated and a new session is created.
    - If the subscriber profile has not changed, the provisioned policies for active services are verified to determine whether they are affected by the updated attachment information.
12. Any changes are applied to the service node. If no policies have changed but the subscriber identity is different, the SAE changes the subscriber identity on the service node.
13. The subscriber activates a service through the ASG.
14. The ASG creates a service session in the SSR.
15. The SSR notifies all SAEs that a new service session exists.
16. The SAE that manages PTSP sessions for the attachment session activates a service session for the appropriate subscriber session.

Changing the Network Connection

The CPE connects to the network by different means. The attachment session is modified without changing the IP layer. The sequence of events is:

1. The CPE connects to the network through the access device in a different manner. For example, a wireless device roams to a different access point.
2. The access device notifies the access manager about the modified session parameters.
3. The access manager forwards the notification to the SIC.
4. The SIC updates the attachment session in the SSR.
5. The SSR notifies the SAE that the attachment session has been modified. The SAE finds any affected subscriber sessions. The SSR notifies all active SAEs in the same cluster.
6. For any affected subscriber session, the SAE updates the classification context and initiates a login. This login runs the subscriber classification script and compares the result.
    - If the subscriber profile has changed, the existing session is terminated and a new session is created.
    - If the subscriber profile has not changed, the provisioned policies for active services are verified to determine whether they are affected by the updated attachment information.
7. Any changes are applied to the service node. If no policies have changed but the subscriber identity is different, the SAE installs a policy on the service node with the changed subscriber identity.

If the IP layer is modified, the existing attachment session is terminated and a new attachment session is created.

Disconnecting from the Network

The network connection is terminated. The sequence of events for attachment session termination is:

1. The CPE disconnects from the network.
2. The access device notifies the access manager.
3. The access manager forwards the notification to the SIC.
4. The SIC terminates the attachment session in the SSR.
5. The SSR notifies the SAE.
6. The SAE terminates the subscriber session.
7. The SAE terminates the PTSP session on the service node.

Terminating the PTSP Session

The service node detects the end of the PTSP session because of an idle timeout. The sequence of events for PTSP session termination is:

1. The service node detects an idle timeout, terminates the PTSP session, and notifies the SAE.
2. The SAE terminates any subscriber session associated with the PTSP session, which terminates any service session and generates final accounting information.

PTSP session termination does not affect the attachment session.

If the attachment session remains active and the CPE accesses the network again, the sequence of events is the same as connecting to the network without a PTSP session.

If the attachment session terminates, the SAE receives a notification and terminates any remaining PTSP sessions associated with the attachment session. If there are no associated PTSP sessions, the SAE ignores the event.

Related Documentation

- Service Nodes in an SRC Environment Overview on page 7

PART 2

Configuration

- Configuration Tasks for Managing Service Nodes on page 17

CHAPTER 3

Configuration Tasks for Managing Service Nodes

- Configuring SRC Software to Support Service Nodes on page 17

Configuring SRC Software to Support Service Nodes

To configure the SRC components to support service nodes:

1. Configure the SRC software to communicate with the PTSP peer on the MX Series router, manage the MX Series router, and manage subscriber policies.

   See *Configuring PTSP to Manage Subscriber-Level Policies*.

2. Configure the SIC to listen for RADIUS accounting events from IP edge devices and filter events based on attachment session attributes.

   See *Subscriber Information Collector Overview*.

3. Configure the SSR to store information about IP edge attachment sessions.

   See *Configuring the Initial SSR Cluster (SRC CLI)*.

4. (Optional) Configure Dynamic Service Activator methods for all subscriber sessions.

   See *Enabling Dynamic Service Activator on a Web Application Server (SRC CLI)*.

PART 3

Index

- Index on page 21

Index

C

conventions
- notice icons....x
- text....x

customer support....xii
- contacting JTAC....xii

D

directory
- description....4

directory server....4

documentation
- comments on....xii

L

LDAP (Lightweight Directory Access Protocol). *See* directory; directory server

M

manuals
- comments on....xii

N

notice icons....x

S

SRC components
- description....3

support, technical *See* technical support

T

technical support
- contacting JTAC....xii

text conventions....x

