Network Configuration Example

Configuring Service Provider Wi-Fi

Modified: 2017-01-18

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

Network Configuration Example Configuring Service Provider Wi-Fi

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

Chapter 1 **Configuring Service Provider Wi-Fi 5**

About This Network Configuration Example 5
Service Provider Wi-Fi Drivers 5
Mobile Provider Challenges 5
Wireline Provider Challenges 6
Juniper Networks Proposed Solutions 6
Summary 7
Service Provider Wi-Fi Services Supporting Open and Secure Access 7
Operation of Open Wi-Fi Access Using a Captive Portal 7
Operation of Secure Wi-Fi Access Using EAP Authentication 9
Example: Configuring Open Wi-Fi Access to the Internet Using a Captive Portal and Secure Wi-Fi Access to the Internet Using EAP Authentication 11

CHAPTER 1

Configuring Service Provider Wi-Fi

- About This Network Configuration Example on page 5
- Service Provider Wi-Fi Drivers on page 5
- Service Provider Wi-Fi Services Supporting Open and Secure Access on page 7
- Example: Configuring Open Wi-Fi Access to the Internet Using a Captive Portal and Secure Wi-Fi Access to the Internet Using EAP Authentication on page 11

About This Network Configuration Example

This network configuration example presents configuration examples for mobile and fixed-line service providers to use wireless fidelity (Wi-Fi) 802.11 to offload mobile data traffic from the macro cellular network. It also presents step-by-step procedures for configuring the Juniper Networks' service provider Wi-Fi solution and individual network elements to simultaneously deliver both open Wi-Fi access (with a captive portal) as well as secure Wi-Fi access (with EAP-based authentication).

Service Provider Wi-Fi Drivers

Mobile data traffic has been on an exponential growth curve ever since the introduction of smartphones along with third-generation (3G) and fourth-generation (4G) mobile networks. Service providers want to deliver low-cost alternatives to augment existing macro network capacity to deliver a more compelling user experience.

Mobile Provider Challenges

The explosive growth in smartphones, abundance of sophisticated applications, ever increasing need for universal anytime-anywhere connectivity, and the resulting exponential data traffic growth has put severe demands on the mobile networks of today. The severe demands are both in terms of spectrum as well as backhaul and core network capacities. This is a major challenge for mobile operators in terms of ever increasing demands on the licensed spectrum.

For mobile service provider networks, the growth in mobile data traffic is acute. Increased data usage is causing congestion in the macro network, particularly in high-traffic locations. You are probably investing heavily to increase overall network capacity. New Long Term Evolution (LTE) deployments deliver higher spectral efficiencies and typically come with new blocks of spectrum. Cell splitting enables you to increase the density of the network by adding smaller, more tailored cells to meet demand.

You should continue to explore new access network technologies including Wi-Fi.

Wi-Fi networks are complementary to existing radio access network (RAN) technologies like Universal Mobile Telecommunications System (UMTS), High Speed Packet Access (HSPA), and LTE. Wi-Fi technology enables small cell capacity on a different frequency than the macro cellular network. It can be deployed in concert with other small cell technologies and offers a low-cost access technology. Wi-Fi technology is often more flexible to deploy and is typically lower cost than licensed frequency small cell solutions.

The challenge for you as a mobile service provider is to have Wi-Fi behave more like the existing cellular RAN. Ideally subscribers will attach and authenticate as seamlessly to Wi-Fi service as they do to cellular. Subscribers can have access to the same mobile packet services regardless of the radio network in use.

Wireline Provider Challenges

As a wireline service provider you manage a vast network of high-speed low-cost fixed-line connections. While some of the usage, and much of the revenues, have shifted to mobile providers, the fixed network remains the critical element for connecting mobile devices to the mobile core and on to the Internet. As cellular capacity challenges increase, and mobile providers turn towards technologies like Wi-Fi and other small cell solutions, there is an opportunity for fixed-line providers to offer a compelling mobile data offload solution.

Many fixed access providers have been aggressively building out Wi-Fi networks in high-use locations like dense urban areas, stadiums, and airports. As you look to embrace Wi-Fi technologies, there is a commercial opportunity for you to offer your existing Wi-Fi properties as a complementary access technology.

Juniper Networks Proposed Solutions

To address wireless and wireline service provider's challenges and opportunities, Juniper Networks offers a broad collection of products across multiple solution subsystems to address both open and secure Wi-Fi access in a single network architecture.

The Juniper Networks proposed solutions are described in the following items:

- Open Wi-Fi access to the Internet using a captive portal—In this scenario the mobile user needs access to the Internet or the carrier's service complex. Access is open (unencrypted) and uses a captive portal to authenticate the user credentials in the form of a name and password, a credit card instant payment, or by accepting terms of an agreement.

  Portal-based hotspots offer the simplest and most flexible form of user access, supporting the widest range of devices (for example, non-SIM-based devices) and offering access to pay-as-you-go customers. The primary challenge for the service provider is that this open Wi-Fi network is unsecure.

- Secure Wi-Fi access to the Internet using EAP authentication—In this scenario the user needs access to the Internet or the carrier's service complex. Access is secured using the Extensible Authentication Protocol (EAP) mechanisms between the user's equipment and the operator's network. EAP-based access provides a more secure offering that is tightly integrated into the service provider's subscriber management

system. In contrast to a portal-based hotspot, EAP-based access does not require any user action such as opening a browser or filling in credentials on a captive portal page.

Summary

In conclusion, Wi-Fi technology has become a pragmatic and compelling solution for augmenting cellular RAN capacity. It is an effective means of complementing the mobile access network. It offers an opportunity for fixed providers to leverage their assets to deliver a commercially compelling solution to support mobile data usage.

Related Documentation

- Service Provider Wi-Fi Services Supporting Open and Secure Access on page 7
- Example: Configuring Open Wi-Fi Access to the Internet Using a Captive Portal and Secure Wi-Fi Access to the Internet Using EAP Authentication on page 11

Service Provider Wi-Fi Services Supporting Open and Secure Access

This topic describes the operation of two scenarios for providing service provider Wi-Fi access.

Operation of Open Wi-Fi Access Using a Captive Portal

This section describes the scenario for open Wi-Fi access to the Internet using a captive portal. It presents the call flow and explains the role that each device plays in the topology.

Captive portal-based access describes the process where a user is redirected to a webpage prior to any network access being granted. From this webpage the user inputs the appropriate authentication details to be granted access.

The authentication details might include one of the following:

- User credentials. For example, username and password.
- A mobile station international subscriber directory number (MSISDN). For example, a phone number.
- Some form of payment for the session. For example, a credit card or coupon.
- Agreeing to the terms of service for free access.

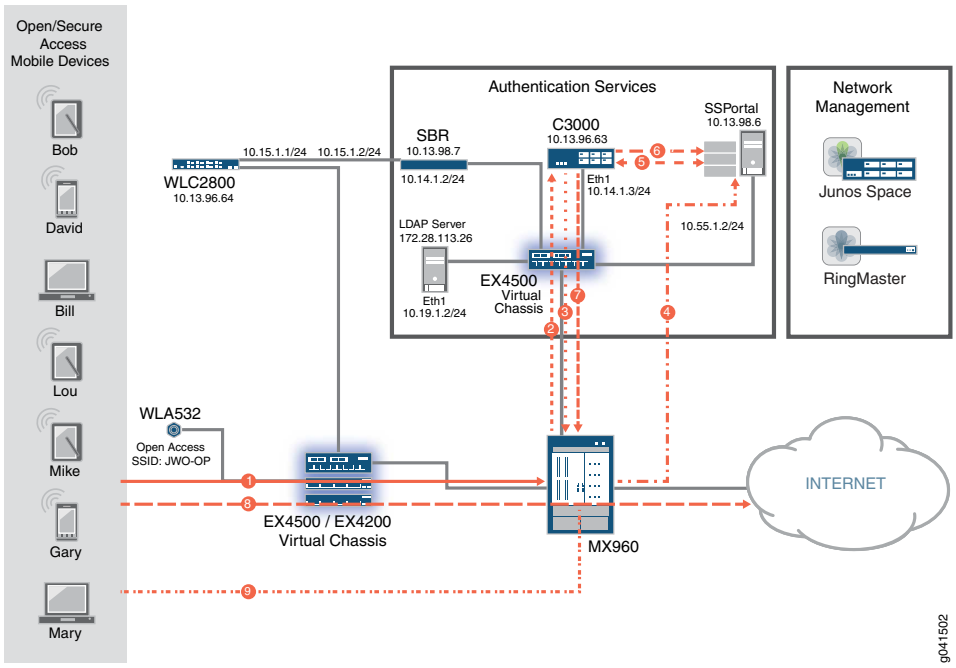
After the requirements of the portal have been met, the user is granted the appropriate level of network access.

In Figure 1 on page 8:

- The Juniper Networks WLA532 Wireless LAN Access Point provides wireless access to the mobile users.
- The Juniper Networks WLC2800 Wireless LAN Controller controls the configuration of the WLAs. It performs configuration, ongoing monitoring, wireless LAN security, wireless LAN user tracking, and authentication on behalf of subscribers.

- The Juniper Networks EX Series Ethernet Switches are configured in a virtual chassis to provide Layer 2 connectivity. Members zero and three of the virtual chassis are EX4500 switches, and member one and two are EX4200 switches.
- The Juniper Networks C3000 Controller is running the Juniper Networks Session and Resource Control (SRC) software to provide session control.
- The SSPortal is a sample residential portal web application. It is used to demonstrate an application that provides a means for subscribers to directly log in to a subscriber session for their ISP. This device also hosts a domain name server for this example.
- The MX960 router provides broadband network gateway (BNG) functionality.
- In your network it is assumed that there is some amount of Layer 2 and Layer 3 infrastructure between the MX Series router and the Internet. In this example, the additional infrastructure is not shown.
- The Juniper Networks Junos Space application and Juniper Networks RingMaster Appliance are shown for reference but are not described in this example.
- The Steel-Belted Radius (SBR) server does not participate in the open access scenario.

Figure 1: Open Wi-Fi Access Operation Using a Captive Portal



The following steps describe the operation of the open scenario in general terms. This is not intended to be an exhaustive engineering specification. Figure 1 on page 8 illustrates these steps:

1. The user's mobile device connects through the WLA532 using the JWO-OP SSID and initiates a DHCP request.
2. The DHCP request triggers the MX Series router to start the provisioning process by sending a JSRC-AA request to the SRC running on the C3000 Controller.
3. Since the subscriber is not present in the Session State Registrar (SSR), the user is an unauthenticated subscriber, and the SRC returns the Open-Portal default profile to the MX Series router. The Open-Portal default profile limits the connection to only a captive portal.
4. The DHCP service running on the MX Series router provides an IPv4 address to the mobile device, the user session is redirected to the captive portal on the sample residential portal (SSPortal) application, and the subscriber provides his user credentials to log in to the portal.
5. The SSPortal verifies the credentials with the C3000 Controller.
6. The user is authenticated.
7. The Internet service policy is sent to the MX Series router by the SRC.
8. The MX Series router applies the Internet service policy to the user session, and the user accesses the Internet.
9. The user session disconnects after the idle timeout period.

Operation of Secure Wi-Fi Access Using EAP Authentication

This section describes the scenario for secure Wi-Fi access to the Internet using EAP authentication. It presents the call flow and explains the role that each device plays in the topology.

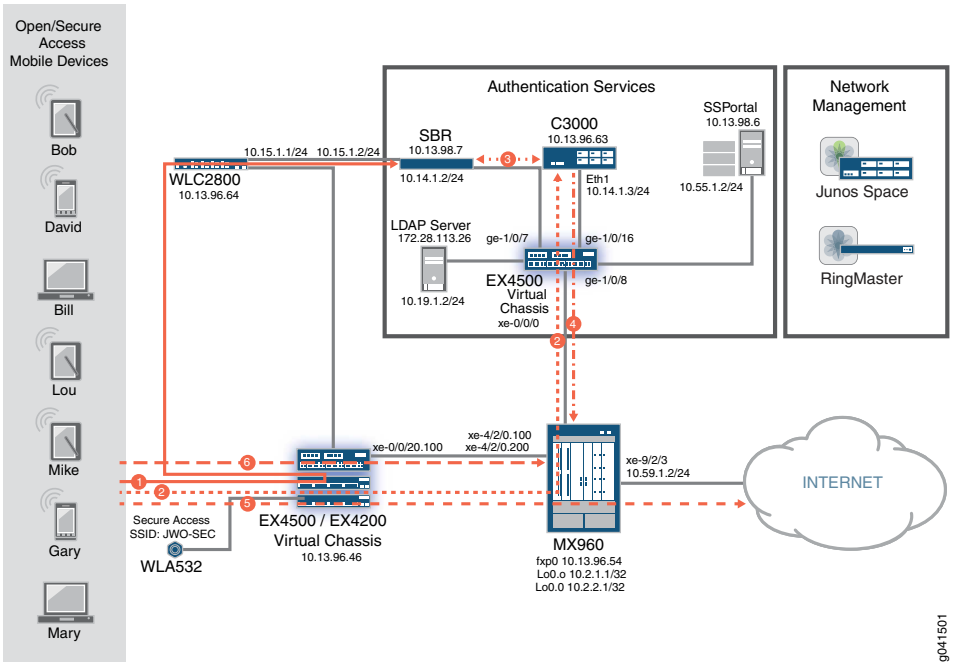
EAP-based access is an automated authentication process between the mobile device and the Authentication, Authorization, and Accounting (AAA) server on the network. Software on the mobile device negotiates with the AAA server and agrees on the manner in which credentials are exchanged with the network. Authentication occurs during the Wi-Fi attachment, and once connected the user has his subscribed network access.

In Figure 2 on page 10:

- The Juniper Networks WLA532 Wireless LAN Access Point provides wireless access to the mobile users.
- The Juniper Networks WLC2800 Wireless LAN Controller controls the configuration of the WLAs.
- The Juniper Networks EX Series Ethernet Switches are configured in a virtual chassis to provide Layer 2 connectivity. Members zero and three of the virtual chassis are EX4500 switches, and member one and two are EX4200 switches.

- The Juniper Networks C3000 Controller is running the Series Session and Resource Control Modules to provide session control.
- The MX960 router provides broadband network gateway (BNG) functionality.
- In your network it is assumed that there is some amount of Layer 2 and Layer 3 infrastructure between the MX Series router and the Internet. In this example, the additional infrastructure is not shown.
- The Steel-Belted Radius (SBR) server provides AAA services.
- The SSPortal does not participate in the secure access scenario.
- The Juniper Networks Junos Space application and Juniper Networks RingMaster Appliance are shown for reference but are not described in this example.

Figure 2: Secure Wi-Fi Access Operation Using EAP Authentication



The following steps describes the operation of the secure scenario in general terms. This is not intended to be an exhaustive engineering specification. Figure 2 on page 10 illustrates these steps:

1. The user's mobile device connects through the WLA532 using the JWO-SEC SSID. The WLC2800 exchanges messages between the mobile device and the SBR AAA server. The mobile device and the SBR AAA server agree on the EAP type (EAP-PEAP in this example), and the mobile device presents credentials. The SBR sends a message to the WLC to allow the mobile device and updates the Session State Registrar (SSR).
2. The WLC forwards the DHCP request from the mobile device to the MX Series BNG, and the MX Series router sends a JSRC-AA request to the SRC running on the C3000 Controller to determine the appropriate policy for the subscriber.

3. The SRC sends a Lightweight Directory Access Protocol (LDAP) request to the SBR that includes the MAC address of the mobile device. The SRC retrieves the username, calling station's ID, and service bundle.
4. The SRC pushes the Internet policy to the MX Series router.
5. The user accesses the Internet.
6. The user session disconnects after the idle timeout period.

Related Documentation

- Service Provider Wi-Fi Drivers on page 5
- Example: Configuring Open Wi-Fi Access to the Internet Using a Captive Portal and Secure Wi-Fi Access to the Internet Using EAP Authentication on page 11

Example: Configuring Open Wi-Fi Access to the Internet Using a Captive Portal and Secure Wi-Fi Access to the Internet Using EAP Authentication

This example provides step-by-step procedures to configure open Wi-Fi access to the Internet using a captive portal and secure Wi-Fi access to the Internet using EAP authentication.

- Requirements on page 11
- Overview on page 12
- Configuration on page 14
- Verification on page 45

Requirements

This example uses the following hardware and software components:

- One Juniper Networks MX Series 3D Universal Edge Router running Junos OS Release 11.4 or later.
- Four Juniper Networks EX4200 Ethernet Switches or EX4500 Ethernet Switches configured as virtual chassis and running Junos OS Release 11.4 or later.
- One Juniper Networks WLC2800 Wireless LAN Controller running Mobility System Software (MSS) Release 7.7 (MR1) or later.
- Two Juniper Networks WLA532 Wireless LAN Access Points. There are no software requirements.
- One Juniper Networks C3000 Controller running Juniper Networks Session and Resource Control (SRC) portfolio Release 4.2.0 R1 or later.
- One SSPortal application running Release 4.2.0 R1 or later running on Oracle Solaris 10 9/10.
- One Steel-Belted Radius (SBR) server running SBR Carrier Standalone Release 7.4.1.R-0.225283 or later on Oracle Solaris 10 9/10.

NOTE: This configuration example has been tested using the software release listed and is assumed to work on all later releases.

Overview

In this example, two WLA532 access points provide Wi-Fi service to mobile users. The WLC2800 controller is the single point of control for the WLAs.

The EX Series switches are configured as a virtual chassis. The first three EX Series switches in the virtual chassis provide Layer 2 connectivity from the WLA532 access points to the WLC2800 Wireless LAN Controller and between the WLC2800 controller and the MX Series router. The fourth EX Series switch in the virtual chassis connects the MX Series router to the C3000 Controller.

The MX Series router is providing Dynamic Host Configuration Protocol (DHCP) services and Juniper Session and Resource Control services.

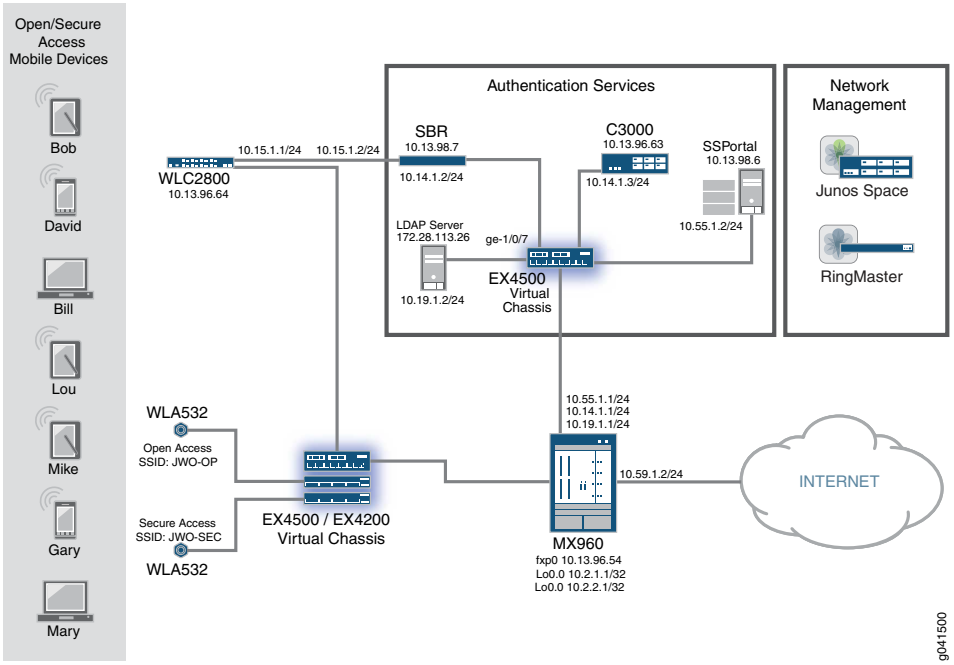
The Steel-Belted Radius server is providing authentication, authorization, and accounting (AAA) services using the Extensible Authentication Protocol (EAP).

The C3000 Controller is providing Session and Resource Control (SRC) services.

The SSPortal is a sample residential portal application provided by Juniper Networks. The sample residential portal application is used for testing purposes in this example.

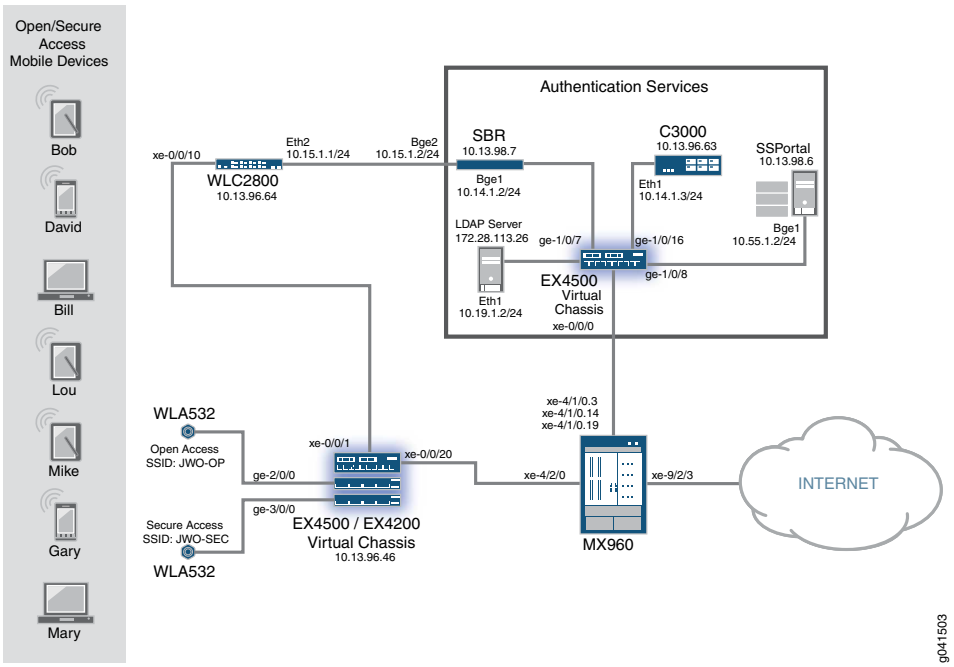
The physical topology is shown in Figure 3 on page 13.

Figure 3: Carrier Wi-Fi Access Supporting Open and Secure Wi-Fi Access Logical Topology



The physical topology is shown in Figure 4 on page 13.

Figure 4: Carrier Wi-Fi Access Supporting Open and Secure Wi-Fi Access Physical Topology



For more information about the operation of this example, see *Service Provider Wi-Fi Drivers* and *Service Provider Wi-Fi Services Supporting Open and Secure Access*.

Configuration

To configure this example, perform the following procedures:

NOTE: In any configuration session it is a good practice to periodically use the commit check command to verify that the configuration can be committed.

- Configuring the Wireless LAN Controller System Settings on page 15
- Configuring the Wireless LAN Controller VLANs on page 16
- Configuring the Wireless LAN Controller Interfaces on page 17
- Configuring the Wireless LAN Controller Service Profiles on page 18
- Configuring the Wireless LAN Controller Radio Profiles on page 19
- Adding the WLA532 Access Points on page 20
- Configuring the Wireless LAN Controller Authentication and Authorization on page 21
- Creating Authentication Profiles on the Wireless LAN Controller on page 21
- Configuring the MX Series Broadband Network Gateway Routing Engines on page 22
- Configuring the MX Series Router Physical, Logical, and Demultiplexing Interfaces on page 22
- Configuring the MX Series Broadband Network Gateway Firewall Filters for Open Access on page 24
- Configuring the MX Series Broadband Network Gateway Web Portal Routing Instance for Open Access on page 25
- Configuring the MX Series Broadband Network Gateway Dynamic Profiles for Open Access on page 26
- Configuring the MX Series Router Local DHCP Services and DHCP Address Assignment Pool on page 27
- Configuring the MX Series Router Diameter Protocol on page 28
- Configuring the MX Series Router JSRC Environment on page 29
- Configuring the MX Series Router Access Profile for the Diameter Protocol on page 29
- Configuring the MX Series Broadband Network Gateway Dynamic Profiles for Secure Access on page 30
- Configuring the MX Series Router Broadband Network Gateway Firewall Filters for Secure Access on page 31
- Configuring the MX Series Broadband Network Gateway Web Portal Routing Instance for Secure Access on page 33
- Configuring the EX Series Switch Physical Interfaces on page 33
- Configuring the SSPortal and Enabling Local Authentication on page 34

- Configuring the C3000 Controller to Provide Series Session and Resource Control for Open Access on page 36
- Configuring the C3000 Controller to Send LDAP Queries to the SBR on page 39
- Adding a Native User to the SBR Server on page 41

Configuring the Wireless LAN Controller System Settings

Step-by-Step Procedure

In this procedure you configure the Juniper Networks WLC2800 Wireless LAN Controller through a serial port. For information about connecting a serial port to the WLC, see the *Wireless LAN Controllers Quick Start Guide*. After each **set** command is entered, the system displays: **success: change accepted**.

Before you begin, physically install the wireless LAN access points, wireless LAN controller, routers, and switches as shown in the physical topology illustration.

NOTE: You must have a basic familiarity with Mobility System Software (MSS), the operating system on the WLC, before you begin configuring it. The CLI hierarchy is different from Junos OS. See the *Mobility System Software Quick Start Guide*.

1. Configure the WLC IPv4 address.

   Specify **10.15.1.1** as the IPv4 address and **255.255.255.0** as the subnet mask. The **10.15.1.1** IPv4 address is used to communicate with the SBR server shown in the example network illustration.

   ```
   WLC# set system ip 10.15.1.1 255.255.255.0
   ```

2. Configure the WLC system name.

   Specify **MOB-WO-64** as the name. The name is useful to distinguish the WLC from other devices on the network.

   ```
   WLC# set system name MOB-WO-64
   ```

3. Configure the WLC country code.

   Specify **US** as the country for this example. Wireless networks are subject to regulatory parameters based on the country code where the WLCs and WLAs are physically located, so you must set the country code.

   ```
   MOB-WO-64# set system countrycode US
   ```

4. Configure the WLC enable password.

   Specify **jollyroger** as the password for this example. The password is necessary to ensure that only administrators with the enable password can make configuration changes.

   ```
   MOB-WO-64# set enable password jollyroger
   ```

5. Configure the admin user to use an encrypted password on the WLC.

Specify **admin** as the user name and **encrypted** as the password type. Specify **default** as the VLAN the **admin** user is associated with. VLAN 1 is named **default** by default. The **encrypted** option indicates that the enable password string you entered is already in its encrypted form.

```
MOB-WO-64# set user admin password encrypted
MOB-WO-64# set user admin attr vlan-name default
```

6. Create a static route to the EX4500 switch.

   Specify **10.13.98.0** as the destination subnet, **255.255.255.0** as the subnet mask, **10.13.96.1** as the next hop router, and **2** as the distance. Also create a static route to the **172.0.0.0** subnet for communication with the network management applications.

   ```
   MOB-WO-64# set ip route 10.13.98.0 255.255.255.0 10.13.96.1 2
   MOB-WO-64# set ip route 172.0.0.0 255.0.0.0 10.13.96.1 1
   ```

7. Enable telnet access to the WLC.

   ```
   MOB-WO-64# set ip telnet server enable
   ```

8. As a best practice, save your configuration before proceeding.

   ```
   MOB-WO-64# save config
   success: change accepted.
   ```

Configuring the Wireless LAN Controller VLANs

Step-by-Step Procedure

In this procedure you configure virtual LANs (VLANs). A VLAN is a Layer 2 broadcast domain that can span multiple wired or wireless LAN segments. When a user successfully authenticates to the network, the user is assigned to a specific VLAN.

Each VLAN is given a VLAN name, associated with a port (interface), and configured with a tag.

NOTE: By default VLAN 1 is assigned the name **default**. If you use a tag value, we recommend that you use the same value as the VLAN number. MSS does not require the VLAN number and tag value to be the same, but other vendors' devices might require it.

1. Configure VLAN 1.

   Specify port **1**. VLAN 1 maps to interface 1 with the IPv4 address 10.13.96.64.

   ```
   MOB-WO-64# set vlan 1 port 1
   ```

2. Configure VLAN 2.

   Specify port **2**. Specify **sbr** as the VLAN name. VLAN 2 maps to interface 2 with the IP address 10.15.1.1. In this example VLAN2 does not require a tag.

   ```
   MOB-WO-64# set vlan 2 name sbr
   MOB-WO-64# set vlan 2 port 2
   ```

3. Configure VLAN 10.

Specify port **10**. Specify **wlan-1** as the VLAN name and specify **10** as the VLAN tag. VLAN 10 maps to interface 10 with the IP address 192.168.10.2.

```
MOB-WO-64# set vlan 10 name wlan-1
MOB-WO-64# set vlan 10 port 10 tag 10
```

4. Configure VLAN 100.

   Specify port **10**. Specify **wo-mx** as the VLAN name, and specify **100** as the VLAN tag. VLAN 100 maps to interface 100 with the IP address 10.2.1.2.

   ```
   MOB-WO-64# set vlan 100 name wo-mx
   MOB-WO-64# set vlan 100 port 10 tag 100
   ```

5. Configure VLAN 20.

   Specify port **10**. Specify **wla-2** as the VLAN name, and specify **20** as the VLAN tag. VLAN 20 maps to interface 20 with the IP address 192.168.20.2.

   ```
   MOB-WO-64# set vlan 20 name wla-2
   MOB-WO-64# set vlan 20 port 10 tag 20
   ```

6. Configure VLAN 200.

   Specify port **10**. Specify **wo-mx-2** as the VLAN name, and specify **200** as the VLAN tag. VLAN 200 maps to interface 200 with the IP address 192.168.20.2.

   ```
   MOB-WO-64# set vlan 200 name wo-mx-2
   MOB-WO-64# set vlan 200 port 10 tag 200
   ```

Configuring the Wireless LAN Controller Interfaces

Step-by-Step Procedure

In this procedure you must configure six separate interfaces on the WLC.

One interface is the management interface with the IP address 10.13.96.64. Two interfaces disable the internal DHCP server on the WLC for a block of IP addresses. This is necessary because the MX Series router is acting as the DHCP server and is providing IP addresses to the WLAs. Two more interfaces are used to send network traffic to the MX Series router.

1. Configure the first interface.

   Specify **10.13.96.64** as the IPv4 address and **255.255.255.0** as the subnet mask.

   ```
   MOB-WO-64# set interface 1 ip 10.13.96.64 255.255.255.0
   ```

2. Configure the second interface.

   Specify **10.15.1.1** as the IPv4 address and **255.255.255.0** as the subnet mask. The second interface communicates with devices on the **10.15.1.0** subnet.

   ```
   MOB-WO-64# set interface 2 ip 10.15.1.1 255.255.255.0
   ```

3. Configure interface 10.

   Specify **10** as the interface number, **192.168.10.2** as the IPv4 address, and **255.255.255.0** as the subnet mask.

   Disable the internal DCHP server for a range of addresses and block out the range of IP addresses used by the MX Series router. Specify **disable** to disable the DHCP

server, specify **192.168.10.10** as the starting address in the range of addresses to block and **192.168.10.254** as the ending address, and specify **192.168.10.1** (EX Series device) as the DHCP client default router.

You must set the default route in this command to prevent the WLC from sending the static route previously configured to the DHCP client to use.

```
MOB-WO-64# set interface 10 ip 192.168.10.2 255.255.255.0
MOB-WO-64# set interface 10 ip dhcp-server disable start 192.168.10.10. stop
  192.168.10.254 default-router 192.168.10.1
```

4. Configure interface 100.

   Specify **100** as the interface number, **10.2.1.2** as the IPv4 address, and **255.255.255.0** as the subnet mask.

   Specify **disable** to disable the DHCP server, and specify **192.168.1.10** as the starting address in the range of addresses to block and **192.168.1.254** as the ending address.

   ```
   MOB-WO-64# set interface 100 ip 10.2.1.2 255.255.255.0
   MOB-WO-64# set interface 100 ip dhcp-server disable start 192.168.1.10. stop
     192.168.1.254
   ```

5. Configure the two interfaces that communicate with the EX Series switch and the MX Series router.

   ```
   MOB-WO-64# set interface 20 ip 192.168.20.2 255.255.255.0
   MOB-WO-64# set interface 200 ip 10.2.2.2 255.255.255.0
   ```

Configuring the Wireless LAN Controller Service Profiles

Step-by-Step Procedure

In this procedure you configure service profiles. A service profile controls advertisement and encryption for a service set identifier (SSID).

1. Configure a service profile to create an encrypted SSID to support the secure access scenario.

   Specify **JWO-EAP** as the profile name and **JWO-SEC** as the SSID name.

   ```
   MOB-WO-64# set service-profile JWO-EAP ssid-name JWO-SEC
   ```

2. Disable the 802.11n short guard interval on the JWO-EAP service profile.

   The short guard interval prevents inter-symbol interference on an 802.11n network. Leaving the short guard interval enabled is appropriate for home-use deployments.

   ```
   MOB-WO-64# set service-profile JWO-EAP 11n short-guard-interval disable
   ```

3. Enable the Wi-Fi Protected Access (WPA) information element in the service profile, and enable Temporal Key Integrity Protocol (TKIP) encryption for Robust Security Network (RSN) or WPA clients.

   ```
   MOB-WO-64# set service-profile JWO-EAP wpa-ie cipher-tkip enable
   MOB-WO-64# set service-profile JWO-EAP wpa-ie enable
   ```

4. Add a VLAN to the service profile.

   Specify **wo-mx-2** as the VLAN name.

   ```
   MOB-WO-64# set service-profile JWO-EAP attr vlan-name wo-mx-2
   ```

5. Configure a service profile to create an open access SSID.

   Specify **Open** as the profile name and **JWO-OP** as the SSID name. Also configure the SSID type as **clear**.

   ```
   MOB-WO-64# set service-profile Open ssid-name JWO-OP
   MOB-WO-64# set service-profile Open ssid-type clear
   ```

6. Configure the open service profile to automatically authenticate the user and allow access to the SSID requested by the user without a username and password.

   Specify **last-resort** as the authentication fall-through behavior.

   ```
   MOB-WO-64# set service-profile Open auth-fallthru last-resort
   ```

7. Disable the 802.11n short guard interval on the open service profile.

   The short guard interval prevents inter-symbol interference on an 802.11n network. Leaving the short guard interval enabled is appropriate for home-use deployments.

   ```
   MOB-WO-64# set service-profile Open 11n short-guard-interval disable
   ```

8. Disable encryption on the open service profile.

   ```
   MOB-WO-64# set service-profile Open wpa-ie auth-dot1x disable
   MOB-WO-64# set service-profile Open rsn-ie auth-dot1x disable
   ```

9. Add the VLAN on the open service profile.

   Specify **wo-mx** as the VLAN name.

   ```
   MOB-WO-64# set service-profile Open attr vlan-name wo-mx
   ```

Configuring the Wireless LAN Controller Radio Profiles

Step-by-Step Procedure

In this procedure you configure radio profiles. A radio profile is a set of parameters that apply to multiple radios. You can assign configuration parameters to many radios by configuring a profile and assigning the profile to the radios. Radio profiles then map to service profiles.

1. Create a radio profile named **JWO-1**.

   ```
   MOB-WO-64# set radio-profile JWO-1
   ```

2. Configure the radio profile channel width.

   Specify **20MHz** as the width.

   ```
   MOB-WO-64# set radio-profile JWO-1 11n channel-width-na 20MHz
   ```

3. Map the radio profile to the **Open** service profile.

   ```
   MOB-WO-64# set radio-profile JWO-1 service-profile Open
   ```

4. Create a radio profile named **JWO-2** and map it to the **JWO-EAP** secure service profile.

   ```
   MOB-WO-64# set radio-profile JWO-2
   MOB-WO-64# set radio-profile JWO-2 11n channel-width-na 20MHz
   MOB-WO-64# set radio-profile JWO-2 service-profile JWO-EAP
   ```

Adding the WLA532 Access Points

Step-by-Step Procedure

In this procedure you configure the WLC2800 to identify the WLA532s by serial number, apply a name and description to the access points, and apply the radio profiles.

1. Disable the automatic Distributed WLA configuration type.

   ```
   MOB-WO-64# set ap auto mode disable
   ```

2. Disable the requirement for encryption keys from the WLA532s.

   ```
   MOB-WO-64# set ap security none
   ```

3. Configure the WLC2800 to identify the first WLA532 connected to port 1 by serial number.

   In this example, specify **1** as the Distributed WLA number, **jb0212247313** as the serial number, and **WLA532-US** as the model number.

   NOTE: In your network, use the serial number located on the back of your WLA for this step.

   ```
   MOB-WO-64# set ap 1 serial-id jb0212247313 model WLA532-US
   ```

4. Configure a name and description for the WLA.

   ```
   MOB-WO-64# set ap 1 name WO-1
   MOB-WO-64# set ap 1 description WiFi Offload
   ```

5. Apply the radio profile for the WLA.

   Specify **1** for the first radio in the WLC532, and specify **2** for the second radio. Specify **JWO-1** as the profile and **enable** as the mode for both radios.

   ```
   MOB-WO-64# set ap 1 radio 1 radio-profile JWO-1 mode enable
   MOB-WO-64# set ap 1 radio 2 radio-profile JWO-1 mode enable
   ```

6. Configure the WLC2800 to identify the second WLA532 connected to port 2.

   NOTE: In your network, use the serial number located on the back of your WLA for this step.

   ```
   MOB-WO-64# set ap 2 serial-id jb0212248475 model WLA532-US
   MOB-WO-64# set ap 2 name WO-2
   MOB-WO-64# set ap 2 description WiFi Offload
   MOB-WO-64# set ap 2 radio 1 radio-profile JWO-2 mode enable
   MOB-WO-64# set ap 2 radio 2 radio-profile JWO-2 mode enable
   ```

Configuring the Wireless LAN Controller Authentication and Authorization

Step-by-Step Procedure

In this procedure you configure the RADIUS client on the WLC.

1. Configure the RADIUS client with the system IPv4 address.

   Doing this causes the RADIUS client to use the IPv4 address specified in the **set system ip-address** command as the source address in the request packets sent to the server.

   ```
   MOB-WO-64# set radius client system-ip
   ```

2. Configure the RADIUS client and attributes.

   Specify **sol.mob.sbr** as the server name. Specify **10.15.1.2** as the IPv4 address of the RADIUS server.

   Specify **5** seconds as the time the RADIUS client waits for a response from the RADIUS server before retransmitting. Specify **3** as the number of transmission attempts before declaring an unresponsive RADIUS server unavailable. Specify **5** as the number of minutes the WLC waits after declaring an unresponsive RADIUS server unavailable before retrying that RADIUS server.

   Specify **09404f0b485744** as the encrypted shared secret key. The key will be different on your network. Specify **USE-MAC-ADDRESS** to send the user MAC address as the password used for authorization to a RADIUS server for MAC authentication.

   ```
   MOB-WO-64# set radius server sol.mob.sbr address 10.15.1.2 timeout 5 retransmit
     3 deadtime 5 encrypted-key 09404f0b485744 author-password
     USE-MAC-ADDRESS
   ```

3. Configure the RADIUS client to use the colon separated format for the MAC address used for the password.

   Specify **colons** as the format.

   ```
   MOB-WO-64# set radius server sol.mob.sbr mac-addr-format colons
   ```

4. Configure the RADIUS client with a server group name and group member name.

   Specify **sol.mob.sbr-group** as the group name and specify **sol.mob.sbr** as a member server name.

   ```
   MOB-WO-64# set server group sol.mob.sbr-group members sol.mob.sbr
   ```

Creating Authentication Profiles on the Wireless LAN Controller

Step-by-Step Procedure

In this procedure you create AAA profiles that use 802.1X authentication.

1. Enable command accounting for the secure users authenticated by the dot1x authentication method.

   Specify **dot1x** to audit the users who are authenticated by the dot1x method. Specify **JWO-SEC** as the SSID name to which this accounting rule applies. Specify ** to match all usernames.

   ```
   MOB-WO-64# set accounting dot1x ssid JWO-SEC ** start stop sol.mob.sbr-group
   ```

2. Enable authentication auditing for the secure users authenticated by the dot1x authentication method.

   Specify **dot1x** to audit the users who are authenticated by the dot1x method. Specify **JWO-SEC** as the SSID name to which this accounting rule applies. Specify ****** to match all usernames.

   ```
   MOB-WO-64# set authentication dot1x ssid JWO-SEC ** pass-through
     sol.mob.sbr-group
   ```

Configuring the MX Series Broadband Network Gateway Routing Engines

Step-by-Step Procedure

In this procedure you configure the MX Series dual Routing Engines using a Junos OS command line interface.

The MX Series router plays a central role in this configuration. The MX Series router is providing Dynamic Host Configuration Protocol (DHCP) services and Juniper Session and Resource Control services. Think of the MX Series router as the gatekeeper for Internet access.

1. Configure a hostname on each Routing Engine.

   ```
   [edit]
   user@host# set groups re0 system host-name sol-mob-54
   user@host# set groups re1 system host-name sol-mob-55
   ```

2. Configure an IP address and protocol family on the **fxp0** management interface for each Routing Engine.

   ```
   [edit]
   user@host# set groups re0 interfaces fxp0 unit 0 family inet address 10.13.96.54/24
   user@host# set groups re1 interfaces fxp0 unit 0 family inet address 10.13.96.55/24
   ```

3. Configure the router to automatically load and commit the configuration on both Routing Engines.

   ```
   [edit]
   user@host# set system commit synchronize
   ```

4. Apply the group configuration for each Routing Engine.

   ```
   [edit]
   user@host# set apply-groups re0
   user@host# set apply-groups re1
   ```

Configuring the MX Series Router Physical, Logical, and Demultiplexing Interfaces

Step-by-Step Procedure

In this procedure you configure the physical and logical interfaces on the MX Series router.

1. Enable VLAN tagging on the **xe-4/1/0** 10-Gigabit Ethernet physical interface and optionally add a description.

   ```
   [edit]
   user@host# set interfaces xe-4/1/0 vlan-tagging
   user@host# set interfaces xe-4/1/0 description "CONNECTED TO EX4500-46"
   ```

2. Configure an IPv4 address and protocol family on the logical interfaces under the **xe-4/1/0** physical interface, specify the **inet** protocol family, and assign a VLAN ID.

```
[edit]
user@host# set interfaces xe-4/1/0 unit 3 family inet address 10.55.1.1/24
user@host# set interfaces xe-4/1/0 unit 3 vlan-id 3
user@host# set interfaces xe-4/1/0 unit 14 family inet address 10.14.1.1/24
user@host# set interfaces xe-4/1/0 unit 14 vlan-id 14
user@host# set interfaces xe-4/1/0 unit 19 family inet address 10.19.1.1/244
user@host# set interfaces xe-4/1/0 unit 19 vlan-id 19
```

3. Enable VLAN tagging on the **xe-4/2/0** 10-Gigabit Ethernet physical interface and optionally add a description.

```
[edit]
user@host# set interfaces xe-4/2/0 vlan-tagging
user@host# set interfaces xe-4/2/0 description "CONNECTED TO EX-AP1"
```

4. Configure logical interface **100** under the **xe-4/2/0** physical interface.

   Specify the **inet** protocol family and configure the interface to use either the preferred **10.2.1.1** address or an unnumbered IPv4 address derived from the **lo0.0** loopback interface. Also assign a VLAN ID.

```
[edit]
user@host# set interfaces xe-4/2/0 unit 100 family inet unnumbered-address lo0.0
   preferred-source-address 10.2.1.1
user@host# set interfaces xe-4/2/0 unit 100 demux-source inet
user@host# set interfaces xe-4/2/0 unit 100 vlan-id 100
```

5. Configure logical interface **200** under the **xe-4/2/0** physical interface.

   Specify the **inet** protocol family and configure the interface to use either the preferred **10.2.2.1** address or an unnumbered IPv4 address derived from the **lo0.0** loopback interface. Also assign a VLAN ID.

```
[edit]
user@host# set interfaces xe-4/2/0 unit 200 family inet unnumbered-address lo0.0
   preferred-source-address 10.2.2.1
user@host# set interfaces xe-4/2/0 unit 200 demux-source inet
user@host# set interfaces xe-4/2/0 unit 200 vlan-id 200
```

6. Create the logical demultiplexing (demux) interface.

   Configure the demux source family address type on the IP demux underlying interface under the **xe-4/2/0** physical interface and unit **100** logical interface. Specify the **inet** family to use IPv4 as the address family for the demux interface source address.

```
[edit]
user@host# set interfaces xe-4/2/0 unit 100 demux-source inet
```

7. Configure the Routing Engine loopback logical interfaces.

   Specify **lo0** as the loopback interface and **0** as the logical interface number. Specify the **inet** address family. Configure the interface to use **10.2.1.1** as the primary IPv4 address and **10.2.2.1** as a secondary address.

```
[edit]
user@host# set interfaces lo0 unit 0 family inet address 10.2.1.1/32 primary
user@host# set interfaces lo0 unit 0 family inet address 10.2.2.1/32
```

Configuring the MX Series Broadband Network Gateway Firewall Filters for Open Access

Step-by-Step Procedure

In this procedure you configure firewall filters on the MX Series router to support the open access scenario. Firewall filters are used in this scenario to redirect the HTTP traffic to the routing instance of the captive Web portal and to account for the traffic that is ICMP, Proxy HTTP, HTTP, or discarded.

1. Create a firewall filter.

   Specify **myifd-xe-4/2/0.100** as the name and include the **interface-specific** option. The **interface-specific** option is used to configure firewall counters that are specific to interfaces. The **inet** address family is applied by default and not explicitly configured.

   ```
   [edit]
   user@host# set firewall filter myifd-xe-4/2/0.100 interface-specific
   ```

2. Configure the first term in the firewall filter.

   Specify **6** as the term name and **icmp** as the protocol to match. Configure the term to count the ICMP packets and write the information to a counter named **icmpcount**. Also configure the terminating action to **accept** the packets.

   ```
   [edit]
   user@host# set firewall filter myifd-xe-4/2/0.100 term 6 from protocol icmp
   user@host# set firewall filter myifd-xe-4/2/0.100 term 6 then count icmpcount
   user@host# set firewall filter myifd-xe-4/2/0.100 term 6 then accept
   ```

3. Configure the second term in the firewall filter.

   Specify **1** as the term name. Configure the term to match packets that are tagged with the **service-filter-hit** action. Also configure the terminating action to **accept** the packets. The packet can be tagged with the **service-filter-hit** action by the RADIUS server.

   The **service-filter-hit** action is used to effectively bypass unnecessary filters when there are filter chains.

   ```
   [edit]
   user@host# set firewall filter myifd-xe-4/2/0.100 term 1 from service-filter-hit
   user@host# set firewall filter myifd-xe-4/2/0.100 term 1 then accept
   ```

4. Configure the third term in the firewall filter.

   This is the term that redirects Web browser traffic to the captive portal.

   Specify **2** as the term name. Configure the term to match the destination TCP port **80** (HTTP). Configure the term to count the packets and write the information to a counter named **port80count**, and then send the packets to the routing instance named **web-portal**.

   ```
   [edit]
   user@host# set firewall filter portal-filter term 2 from destination-port 80
   user@host# set firewall filter portal-filter term 2 then count port80count
   user@host# set firewall filter portal-filter term 2 then routing-instance web-portal
   ```

5. Configure the next term in the firewall filter.

Specify **3** as the term name. Specify **domain** to match packets with the DNS destination TCP port. Also configure the terminating action to **accept** the packets.

```
[edit]
user@host# set firewall filter portal-filter term 3 from destination-port domain
user@host# set firewall filter portal-filter term 3 then accept
```

6. Configure the next term in the firewall filter.

   Specify **4** as the term name. Configure the term to match the destination TCP port **8080** (proxy HTTP). Configure the term to count the packets, write the information to a counter named **port8080count**, and then **accept** the packets.

   ```
   [edit]
   user@host# set firewall filter portal-filter term 4 from destination-port 8080
   user@host# set firewall filter portal-filter term 4 then count port8080count
   user@host# set firewall filter portal-filter term 4 then accept
   ```

7. Configure the final term in the firewall filter.

   Specify **5** as the term name. Configure the term to count the packets, write the information to a counter named **discardcount**, and then **discard** the packets.

   ```
   [edit]
   user@host# set firewall filter portal-filter term 5 then count discardcount
   user@host# set firewall filter portal-filter term 5 then discard
   ```

Configuring the MX Series Broadband Network Gateway Web Portal Routing Instance for Open Access

Step-by-Step Procedure

In this procedure you configure the routing instance that provides the route to the captive Web portal.

1. Download the SSPortal.war file from the following URL:

   ```
   https://download.juniper.net/software/sdx/src-pe-4.4.0/SDK+AppSupport+Demos+Samples.tar.gz
   ```

2. Untar the package and copy the **ssportal.war** file to the deploy directory.

   ```
   user@host> cp
     ../SDK+AppSupport+Demos+Samples/DemosAndSamplesApplications/webapps/ssportal.war
     /export/home0/jboss-6.1.0.Final/server/all/deploy
   ```

3. Configure a routing instance named **web-portal** and specify the **forwarding** instance type.

   ```
   [edit]
   user@host# set routing-instances web-portal instance-type forwarding
   ```

4. Configure a static route that matches all IPv4 addresses and specify **10.55.1.2** as the next hop.

   The 10.55.1.2 address is configured on the Ethernet interface on the SSPortal server.

   ```
   [edit]
   user@host# set routing-instances web-portal routing-options static route 0.0.0.0/0
     next-hop 10.55.1.2
   ```

5. Configure the router to retain the static route in the event that the routing process shuts down.

```
[edit]
user@host# set routing-instances web-portal routing-options static route 0.0.0.0/0
  retain
```

Configuring the MX Series Broadband Network Gateway Dynamic Profiles for Open Access

Step-by-Step Procedure

In this procedure you configure a default dynamic profile on the MX Series router for the open access scenario. Dynamic profiles are 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.

1. Create a dynamic profile and specify the variables.

   Specify **demux-default-open-access** as the name and include the **$junos-interface-unit** variable.

   The variables enable dynamic association of certain interface-specific values to incoming subscriber requests. 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 from configuration. The **$junos-interface-unit** variable is dynamically replaced with the logical interface unit number that DHCP supplies when the subscriber logs in. The **$junos-underlying-interface** variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in. A demux interface uses an underlying logical interface to receive packets.

   ```
   [edit]
   user@host# set dynamic-profiles demux-default-open-access interfaces demux0
     unit "$junos-interface-unit" demux-options underlying-interface
     "$junos-underlying-interface"
   ```

2. Configure the demultiplexing (demux) interface used in the dynamic profile.

   To identify subscribers dynamically, you specify variable values that are dynamically determined when subscribers log in.

   Specify **demux-default-open-access** as the demux interface name. Specify **$junos-interface-unit** as the logical interface variable. Specify **$junos-subscriber-ip-address** as the demux source address variable for a subscriber in the open access dynamic profile. The IPv4 source address for the interface is dynamically supplied by DHCP when the subscriber accesses the router.

   ```
   [edit]
   user@host# set dynamic-profiles demux-default-open-access interfaces demux0
     unit "$junos-interface-unit" family inet demux-source
     $junos-subscriber-ip-address
   ```

3. Configure the demux interface to derive the local source address from the unnumbered IPv4 addresses of the **lo0.0** logical loopback interface.

   ```
   [edit]
   user@host# set dynamic-profiles demux-default-open-access interfaces demux0
     unit "$junos-interface-unit" family inet unnumbered-address lo0.0
   ```

4. Configure the demux interface to dynamically derive the local source address from the preferred source IPv4 address specified.

When you use the dynamic variable, the address that is selected resides in the same network as the IP address of the subscriber, if that address is configured as one of the addresses of the specified interface. Configuring the preferred source address enables you to use an IP address other than the primary IP address on some of the unnumbered Ethernet interfaces in your network.

```
[edit]
user@host# set dynamic-profiles demux-default-open-access interfaces demux0
  unit "$junos-interface-unit" family inet unnumbered-address
  preferred-source-address 10.2.1.1
```

Configuring the MX Series Router Local DHCP Services and DHCP Address Assignment Pool

Step-by-Step Procedure

In this procedure you configure a local DHCP service for each group of clients. The subscriber access feature requires that a subscriber such as a DHCP client send a discover message to the router interface to initialize dynamic configuration of that interface.

You also configure a local DHCP server address assignment pool. The address pool can be used by different client applications.

1. Create a DHCP server group named **Open-Subs**.

   Specify that the DHCP local server is enabled on the dynamic profile named **demux-default-open-access**, the **xe-4/2/0** interface, and the **100** VLAN identifier.

   ```
   [edit]
   user@host# set system services dhcp-local-server group Open-Subs dynamic-profile
     demux-default-open-access
   user@host# set system services dhcp-local-server group Open-Subs interface
     xe-4/2/0.100
   ```

2. Create a DHCP address pool.

   Specify **Open-Dhcp-Pool** as the pool name. Specify the **inet** family and the **10.2.1.0** subnet. Also specify the subnet mask length.

   ```
   [edit]
   user@host# set access address-assignment pool Open-Dhcp-Pool family inet
     network 10.2.1.0/24
   user@host# set access address-assignment pool Open-Dhcp-Pool family inet
     mask-length 32
   ```

3. Specify the upper and lower range of addresses that can be used in the pool.

   ```
   [edit]
   user@host# set access address-assignment pool Open-Dhcp-Pool family inet range
     r1 low 10.2.1.10
   user@host# set access address-assignment pool Open-Dhcp-Pool family inet range
     r1 high 10.2.1.100
   ```

4. Specify the domain name system (DNS) name server available to the client to resolve hostname-to-client mappings.

   In this example the DNS name server is hosted on the same device as the SSPortal.

   This is equivalent to DHCP option 6. It tells the client the DNS servers it can use.

```
[edit]
user@host# set access address-assignment pool Open-Dhcp-Pool family inet
  dhcp-attributes name-server 10.55.1.2
```

5. Specify a router located in the client's subnet.

   This statement is the equivalent of DHCP option 3. It tells the client a router it can use.

```
[edit]
user@host# set access address-assignment pool Secure-Dhcp-Pool family inet
  dhcp-attributes router 10.2.2.1
```

Configuring the MX Series Router Diameter Protocol

Step-by-Step Procedure

In this procedure you configure the Diameter protocol. The Diameter protocol provides communications between the local Service and Resource Control (SRC) peer on a Juniper Networks routing platform and the remote SRC peer on a Juniper Networks C Series Controller.

1. Configure the origin realm used in protocol messages.

   Specify **mob.jnpr.net** as the realm name. Specify **sol-mob-54** as the hostname sent in protocol messages. The hostname is supplied as the value for the Origin-Host AVP by the Diameter instance. The name is used by the administrator. It is not resolved by DNS.

```
[edit]
user@host# set diameter origin realm mob.jnpr.net
user@host# set diameter origin host sol-mob-54
```

2. Configure the Diameter protocol peer.

   Specify **mob-src-63** as the peer name. Specify **1** as the peer priority. A peer with a lower number has a higher priority. Also configure **10.14.1.3** as the peer address and **3868** as the TCP port used for active connections to the peer.

```
[edit]
user@host# set diameter network-element dne1 peer mob-src-63 priority 1
user@host# set diameter peer mob-src-63 address 10.14.1.3
user@host# set diameter peer mob-src-63 connect-actively port 3868
```

3. Define which destinations are reachable through the Diameter network element.

   Specify **route1** as the name of the route. Specify **jsrc** as the name of the application (function) associated with this Diameter network element and **default** as the partition associated with the function. Also specify **mob.jnpr.net** as the destination realm, **dne1** as the destination hostname, and **1** as the route metric.

```
[edit]
user@host# set diameter network-element dne1 forwarding route route1 function
  jsrc
user@host# set diameter network-element dne1 forwarding route route1 function
  partition default
user@host# set diameter network-element dne1 forwarding route route1 destination
  realm mob.jnpr.net
```

```
user@host# set diameter network-element dne1 forwarding route route1 destination
    host dne1
user@host# set diameter network-element dne1 forwarding route route1 metric 1
```

Configuring the MX Series Router JSRC Environment

Step-by-Step Procedure

In this procedure you configure the Juniper Networks Session and Resource Control environment. JSRC and is part of the AAA application running on the MX Series router. JSRC provides a central administrative point for managing subscribers and their services. JSRC works within a specific logical system:routing instance context, called a partition. JSRC is not an acronym.

1. Create a JSRC partition.

   Specify **default** as the partition name and **master** as the routing instance name.

   ```
   [edit]
   user@host# set jsrc-partition default
   user@host# set jsrc partition default diameter-instance master
   ```

2. Specify **mob.jnpr.net** as the destination realm used in protocol messages, and specify **dne1** as the hostname of the destination host that is the service activation engine (SAE).

   ```
   [edit]
   user@host# set jsrc partition default destination-realm mob.jnpr.net
   user@host# set jsrc partition default destination-host dne1
   ```

Configuring the MX Series Router Access Profile for the Diameter Protocol

Step-by-Step Procedure

In this procedure you configure an access profile for open access. The access profile defines the AAA services and options for subscribers associated with the domain map.

1. Configure the authentication order.

   Specify **JWO-P1** as the profile name and specify **none** to grant authentication without examining the client credentials. Configure the provisioning order and specify **jsrc** as the application used to communicate with the SAE for subscriber service provisioning.

   ```
   [edit]
   user@host# set access profile JWO-P1 authentication-order none
   user@host# set access profile JWO-P1 provisioning-order jsrc
   ```

2. Configure the session options using one of the following two methods.

   - Specify **10** minutes as the grace period that begins after an authenticated user terminates all sessions and connections. Authentication is not required if a new connection is initiated by the same user during the grace period. Configure the accounting order and specify **activation-protocol** as the method used for reporting subscriber service accounting. The **activation-protocol** statement causes the router to send service accounting reports by means of the application that activates the services. In this case the service is JSRC.

     ```
     [edit]
     user@host# set access profile JWO-P1 session-options client-idle-timeout 10
     ```

```
user@host# set access profile JWO-P1 service accounting-order
  activation-protocol
```

- If you do not want an authenticated user to be able to reconnect during the grace period, use this alternate configuration. Instead of including the **client-idle-timeout** statement, include the **client-session-timeout** statement. Specify **2** minutes as the timeout. A user session that is idle for more than 2 minutes is disconnected.

  ```
  [edit]
  user@host# set access profile JWO-P1 session-options client-session-timeout 2
  ```

3. Define the access profile to use in the master routing instance by specifying **JWO-P1** as the profile name

   ```
   [edit]
   user@host# set access-profile JWO-P1
   ```

Configuring the MX Series Broadband Network Gateway Dynamic Profiles for Secure Access

Step-by-Step Procedure

In this procedure you configure dynamic profiles on the MX Series router. Dynamic profiles are 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.

1. Create a dynamic profile and specify the variables.

   Specify **Secure-EAP** as the name and include the **$junos-interface-unit** variable.

   The variables enable dynamic association of certain interface-specific values to incoming subscriber requests. 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 from the configuration. The **$junos-interface-unit** variable is dynamically replaced with the logical interface unit number that DHCP supplies when the subscriber logs in. The **$junos-underlying-interface** variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in.

   ```
   [edit]
   user@host# set dynamic-profiles Secure-EAP interfaces demux0 unit
     "$junos-interface-unit" demux-options underlying-interface
     "$junos-underlying-interface"
   ```

2. Configure the logical demux source address for a subscriber in the secure access dynamic-profile.

   Specify **Secure-EAP** as the demux interface name. Specify **$junos-interface-unit** as the logical interface variable. Specify **$junos-subscriber-ip-address** as the demux source address variable for a subscriber in the open access dynamic profile. The IPv4 source address for the interface is dynamically supplied by DHCP when the subscriber accesses the router.

   ```
   [edit]
   user@host# set dynamic-profiles Secure-EAP interfaces demux0 unit
     "$junos-interface-unit" family inet demux-source $junos-subscriber-ip-address
   ```

3. Configure the firewall filter used to evaluate packets that are received on the logical demux interface.

   Specify **jwo-int** as the firewall filter name.

   ```
   [edit]
   user@host# set dynamic-profiles Secure-EAP interfaces demux0 unit
     "$junos-interface-unit" family inet filter input jwo-int
   ```

4. Configure the demux interface to derive the local source address from the unnumbered IPv4 address of the lo0.0 logical loopback interface.

   ```
   [edit]
   user@host# set dynamic-profiles Secure-EAP interfaces demux0 unit
     "$junos-interface-unit" family inet unnumbered-address lo0.0
   ```

5. Configure the demux interface to dynamically derive the local source address from the preferred source IPv4 address specified.

   When you use the dynamic variable, the address that is selected resides in the same network as the IP address of the subscriber, if that address is configured as one of the addresses of the specified interface. Configuring the preferred source address enables you to use an IP address other than the primary IP address on some of the unnumbered Ethernet interfaces in your network.

   ```
   [edit]
   user@host# set dynamic-profiles Secure-EAP interfaces demux0 unit
     "$junos-interface-unit" family inet unnumbered-address preferred-source-address
     10.2.2.1
   ```

Configuring the MX Series Router Broadband Network Gateway Firewall Filters for Secure Access

Step-by-Step Procedure

In this procedure you configure firewall filters on the MX Series router to support the secure access scenario. Firewall filters are used in this scenario to redirect the HTTP traffic to the routing instance that provides connection to the Internet and to account for the traffic that is ICMP, Proxy HTTP, HTTP, or discarded.

1. Create a firewall filter.

   Specify **jwo-int** as the name and include the **interface-specific** option. The **interface-specific** option is used to configure firewall counters that are specific to interfaces. The **inet** address family is applied by default and is not explicitly configured.

   ```
   [edit]
   user@host# set firewall filter jwo-int interface-specific
   ```

2. Configure the first term in the firewall filter.

   Specify **t5** as the term name and **icmp** as the protocol to match. Configure the term to count the packets and write the information to the **service-accounting** counter. Also configure the terminating action to **accept** the packets. When the match conditions for the filter are met, the packet is counted and applied to the well-known service counter (__junos-dyn-service-counter) for use by the RADIUS server.

   ```
   [edit]
   ```

```
user@host# set firewall filter jwo-int term t5 from protocol icmp
user@host# set firewall filter jwo-int term t5 then service-accounting
user@host# set firewall filter jwo-int term t5 then accept
```

3. Configure the second term in the firewall filter.

   Specify **t1** as the term name. Configure the term to match packets that are tagged with the **service-filter-hit** action. Configure the term to count the packets and write the information to the **service-accounting** counter. Also configure the terminating action to **accept** the packets. The packet can be tagged with the **service-filter-hit** action by the RADIUS server.

   The **service-filter-hit** action is used to effectively bypass unnecessary filters when there are filter chains.

   ```
   [edit]
   user@host# set firewall filter jwo-int term t1 from service-filter-hit
   user@host# set firewall filter jwo-int term t1 then service-accounting
   user@host# set firewall filter jwo-int term t1 then accept
   ```

4. Configure the third term in the firewall filter.

   This is the term that directs Web browser traffic to the Internet.

   Specify **t2** as the term name. Configure the term to match the destination TCP port **80** (HTTP). Configure the term to count the packets and write the information to the **service-accounting** counter. Then configure the term to send the packets to the routing instance named **jwo-isp**.

   ```
   [edit]
   user@host# set firewall filter jwo-int term t2 from destination-port 80
   user@host# set firewall filter jwo-int term t2 then service-accounting
   user@host# set firewall filter jwo-int term t2 then routing-instance jwo-isp
   ```

5. Configure the next term in the firewall filter.

   Specify **t4** as the term name. Specify **domain** to match packets with the DNS destination TCP port. Configure the term to count the packets and write the information to the **service-accounting** counter. Also configure the terminating action to **accept** the packets.

   ```
   [edit]
   user@host# set firewall filter jwo-int term t4 from destination-port domain
   user@host# set firewall filter jwo-int term t4 then service-accounting
   user@host# set firewall filter jwo-int term t4 then accept
   ```

6. Configure the final term in the firewall filter.

   Specify **t6** as the term name. Configure the term to match the destination TCP port **8080** (proxy HTTP). Configure the term to count the packets and write the information to the **service-accounting** counter. Also configure the terminating action to **accept** the packets.

   ```
   [edit]
   user@host# set firewall filter jwo-int term t6 from destination-port 8080
   user@host# set firewall filter jwo-int term t6 then service-accounting
   user@host# set firewall filter jwo-int term t6 then accept
   ```


Configuring the MX Series Broadband Network Gateway Web Portal Routing Instance for Secure Access

Step-by-Step Procedure

In this procedure you configure the routing instance that provides the route to the Internet.

1. Configure a routing instance named **jwo-isp** and specify the **forwarding** instance type.

```
[edit]
user@host# set routing-instances jwo-isp instance-type forwarding
```

2. Configure a static route that matches all IPv4 addresses and specify **10.55.1.1** as the next hop on the route to the Internet.

```
[edit]
user@host# set routing-instances jwo-isp routing-options static route 0.0.0.0/0
  next-hop 10.59.1.1
```

3. Configure the router to retain the static route in the event that the routing process shuts down.

```
[edit]
user@host# set routing-instances jwo-isp routing-options static route 0.0.0.0/0
  retain
```

Configuring the EX Series Switch Physical Interfaces

Step-by-Step Procedure

In this procedure you configure the interfaces on the EX Series switch.

NOTE: The interfaces shown in the physical topology illustrations are already configured for Ethernet switching by default. Interfaces ge-2/0/0, ge-3/0/0, ge-1/0/7, ge-1/0/8, and ge-1/0/16 require no additional configuration.

1. Enable port trunking operation on the **xe-0/0/20** interface that is connected to the MX Series router.

   Optionally add a description.

```
[edit]
user@host# set interfaces xe-0/0/20 unit 0 family ethernet-switching port-mode
  trunk
user@host# set interfaces xe-0/0/20 description "CONNECTED TO MX 54"
```

2. Enable port trunking operation and configure a native VLAN identifier on the **xe-0/0/1** interface that is connected to the WLC controller.

   Specify VLAN ID **10**. Optionally add a description.

```
[edit]
user@host# set interfaces xe-0/0/1 unit 0 family ethernet-switching port-mode
  trunk
user@host# set interfaces xe-0/0/1 unit 0 family ethernet-switching native-vlan-id
  10
```

```
user@host# set interfaces xe-0/0/1 description "CONNECTED TO WLC 64 PORT
  10"
```

3. To aid in troubleshooting, add a description to the **ge-2/0/0** and **ge-3/0/0** interfaces.

```
[edit]
user@host# set interfaces ge-2/0/0 description "CONNECTED TO AP 1"
user@host# set interfaces ge-3/0/0 description "CONNECTED TO AP 2"
```

4. Enable port trunking operation on the **xe-0/0/0** interface that is connected to the MX Series router.

```
[edit]
user@host# set interfaces xe-0/0/0 unit 0 family ethernet-switching port-mode
  trunk
```

Configuring the SSPortal and Enabling Local Authentication

Step-by-Step Procedure

In this procedure you configure the SSPortal sample residential portal Web application and enable local authentication. The sample residential portal application is for testing purposes.

NOTE: You can access the software for the SRC sample and demonstration applications, associated documentation for some of the applications, component software to support applications, the SRC SDK, and the product Release Notes on the Juniper Networks Web site at: https://www.juniper.net/support/products/src/index.html#sw .

Before configuring the SSPortal application, install the application. To install the application, see the *SRC PE Software Sample Applications Guide* and the *SRC PE Software Getting Started Guide*.

1. Login as root or another authorized user.
2. Configure the application to redirect the open access users to the Instant Virtual Extranet (IVE) sign-in page.

   Edit the **/opt/UMC/redir/etc/redir.properties** file. Add the line shown in the following example. Specify **10.55.1.2** as the IVE hostname. In operation, the **%(url)s** string is replaced by the requested URL.

```
redir.url = http://10.55.1.2:8080/login.do?url=%(url)s
```

3. Enable local authentication for the open access users.

   Add the lines shown in the following example to the end of the **/export/home0/jboss-6.1.0.Final/server/all/conf/login-config.xml** file:

```
<application-policy name="SSPortalLocalAuth">
    <authentication>
     <login-module code="org.jboss.security.auth.spi.UsersRolesLoginModule"

      flag="required">
       <module-option name = "unauthenticatedIdentity">guest</module-option>
```

```
        <module-option
name="usersProperties">props/SSPortalLocalAuth-users.properties</module-option>

        <module-option
name="rolesProperties">props/SSPortalLocalAuth-roles.properties</module-option>

      </login-module>
    </authentication>
</application-policy>
```

4. Create the SSPortal local authentication roles properties file to add user roles to the portal server.

   Create a file named **/export/home0/jboss-6.1.0.Final/server/all/conf/props/SSPortalLocalAuth-roles.properties**.

   Add the lines shown in the following example to the file:

   ```
   BOB=weblocal
   BILL=weblocal
   MARY=weblocal
   GARY=weblocal
   DAVID=weblocal
   MIKE=weblocal
   PAUL=weblocal
   LOU=weblocal
   SCOTT=weblocal
   KEVIN=weblocal
   JEFF=weblocal
   ```

5. Create the SSPortal local authentication users properties file.

   This file identifies where usernames and passwords are stored.

   Create a file named **/export/home0/jboss-6.1.0.Final/server/all/conf/props/SSPortalLocalAuth-users.properties**.

   Add the lines shown in the following example to the file:

   ```
   BOB=password
   BILL=password
   MARY=password
   GARY=password
   DAVID=password
   MIKE=password
   PAUL=password
   LOU=password
   SCOTT=password
   KEVIN=password
   JEFF=password
   CARL=password
   ```

6. Uncompress the **/webapp/ssportal.war** file.

   The file is normally located under the **/export/home0/jboss-6.1.0.Final/server/all/deploy** directory.

   ```
   root@host# unzip -quo ssportal.war
   ```

7. Add portal behavior session properties to configure the portalBehavior servlet.

   Add the **10.56.1.1** IPv4 address of the LDAP server to the **/ssportal/WEB-INF/portalBehavior.properties** file.

```
Factory.behavior = net.juniper.smgt.ssp.model.ISPServiceBehavior
Config.java.naming.provider.url = ldap://10.56.1.1:389/
Logger.file-1.filter = !ConfigMgr,!DES,/debug-
```

8. Add session information to the Jboss configuration file and enable local authentication.

   Edit the **/ssportal/WEB-INF/jboss-web.xml** file. Add the bold text shown in the following example:

   ```
   <jboss-web>
       <context-root>/ssportal</context-root>
       <security-domain>java:/jaas/SSPortalLocalAuth</security-domain>
   </jboss-web>
   ```

9. Recompress the **ssportal.war** file.

   ```
   root@host# zip -u ssportal.war
   ```

10. Copy the **ssportal.war** file to the **/export/home0/jboss-6.1.0.Final/server/all/deploy** directory.

    This examples assumes you have installed the JavaBeans Open Source Software Application Server (JBoss) in the default directory. If you installed JBoss in a different directory, you need to copy the **ssportal.war** file to the directory where JBoss is installed.

    ```
    root@host> cp ssportal.war /export/home0/jboss-6.1.0.Final/server/all/deploy
    ```

Configuring the C3000 Controller to Provide Series Session and Resource Control for Open Access

Step-by-Step Procedure

In this procedure you configure the C3000 Controller to provide series session and resource control (SRC) for both the open access scenario and the secure access scenario.

1. Configure the controller to provide the Open-Portal profile for the open access scenario.

   Specify **JWO-P1** as the folder name, **OpenAccess-Policy** as the group name, and **PR** as the list name.

   Specify **both** to configure the applicability as ingress and egress interfaces. Specify **junos-ise** to configure the policy role and **Open-Portal** as the name of the dynamic profile.

   ```
   [edit]
   root@mob-src-63> set policies folder JWO-P1 group OpenAccess-Policy list PR
     applicability both
   root@mob-src-63> set policies folder JWO-P1 group OpenAccess-Policy list PR role
     junos-ise
   root@mob-src-63> set policies folder JWO-P1 group OpenAccess-Policy list PR rule
     CR type junos-ise
   root@mob-src-63> set policies folder JWO-P1 group OpenAccess-Policy list PR rule
     CR dynamic-profile profile-name Open-Portal
   ```

2. Configure the controller to provide the Internet profile for the secure access scenario.

Specify **both** to configure the applicability as ingress and egress interfaces. Specify **junos-ise** to configure the policy role and **Internet** as the name of the dynamic profile.

```
[edit]
root@mob-src-63> set policies folder JWO-P1 group Internet-Policy list PR
  applicability both
root@mob-src-63> set policies folder JWO-P1 group Internet-Policy list PR role
  junos-ise
root@mob-src-63> set policies folder JWO-P1 group Internet-Policy list PR rule CR
  accounting
root@mob-src-63> set policies folder JWO-P1 group Internet-Policy list PR rule CR
  type junos-ise
root@mob-src-63> set policies folder JWO-P1 group Internet-Policy list PR rule CR
  dynamic-profile profile-name Internet
```

3. Configure the policy group that is applied when the service is activated.

   Specify **OpenSrv** as the name of the service. Specify **available** to enable a subscriber to activate a service. Specify **/JWO-P1/OpenAccess-Policy** as the name of the policy group. Specify **active** to enable the service. Specify the **normal** type of service.

   ```
   [edit]
   root@mob-src-63> set services global service OpenSrv available
   root@mob-src-63> set services global service OpenSrv policy-group
     /JWO-P1/OpenAccess-Policy
   root@mob-src-63> set services global service OpenSrv status active
   root@mob-src-63> set services global service OpenSrv type normal
   ```

4. Configure the controller to add normal services to the global service scope.

   Specify **InternetSrv** as the name of the service. Specify **600** as the idle timeout after which the SAE deactivates service on the input interface. Specify **available** to enable a subscriber to activate a service. Specify **portals** as the category of the service. Specify **/JWO-P1/Internet-Policy** as the name of the policy group. Specify **active** to enable the service. Specify **vta** as the tracking plugin used to collect accounting data for the service. Specify the **normal** type of service.

   ```
   [edit]
   root@mob-src-63> set services global service InternetSrv accounting-interim-interval
     600
   root@mob-src-63> set services global service InternetSrv available
   root@mob-src-63> set services global service InternetSrv category portals
   root@mob-src-63> set services global service InternetSrv idle-timeout-input 600
   root@mob-src-63> set services global service InternetSrv policy-group
     /JWO-P1/Internet-Policy
   root@mob-src-63> set services global service InternetSrv status active
   root@mob-src-63> set services global service InternetSrv tracking-plug-in vta
   root@mob-src-63> set services global service InternetSrv type normal
   ```

5. Configure the controller network information collector (NIC) to locate the SAE managing a particular subscriber session.

   Specify **OnePopLogin** as the name of the NIC scenario.

   ```
   [edit]
   root@mob-src-63> set slot 0 nic scenario-name OnePopLogin
   ```

6. Configure the router initialization scripts.

Specify **POP-ID** as the name of the SAE group. Specify **""** as the extension class path to router initialization scripts that are not in the default location, **/opt/UMC/sae/lib**. Specify **iorPublisher** as the router initialization script for devices running Junos OS (junos, junos-ise).

The **IorPublisher** script publishes the interoperable object reference (IOR) of the SAE in the directory so that a NIC can associate a router with an SAE.

```
[edit]
root@mob-src-63> set shared sae group POP-ID configuration driver scripts
  extension-path ""
root@mob-src-63> set shared sae group POP-ID configuration driver scripts junos
  iorPublisher
root@mob-src-63> set shared sae group POP-ID configuration driver scripts junos-ise
  iorPublisher
```

7. Configure the external plug-in for the SAE that communicates with the agent.

   Specify **nic** as the name of the SAE group. Specify **external** and **attributes** to configure attributes that are sent to the external plug-in for a NIC host. Specify the plug-in attributes.

   ```
   [edit]
   root@mob-src-63> set shared sae group POP-ID configuration plug-ins name nic
     external attributes [ session-id host router-name interface-name user-ip-address
     login-name domain user-dn if-index user-type primary-user-name ]
   ```

8. Configure the CORBA object reference for the external plug-in.

   The SAE plug-in agents share events with the single SAE plug-in.

   Specify **nic** as the name of the SAE group. Specify **localhost** as the hostname of the machine on which you installed the NIC host that supports the agent. Specify **2809** as the port number on which the name server runs. Specify **nicsae/saePort** as the plug-in name under which the agent is registered in the naming service.

   ```
   [edit]
   root@mob-src-63> set shared sae group POP-ID configuration plug-ins name nic
     external corba-object-reference
     "corbaname::localhost:2809/NameService#nicsae/saePort"
   ```

9. Configure the Enterprise JavaBean (EJB) adapter plug-in.

   When an event that activates a service occurs (for example, a subscriber logs in), the SAE sends a session start event to the SRC Volume-Tracking Application (VTA) through the EJB adaptor plug-in you configure on the SAE.

   Specify **vta** as the name of the SAE group. Specify **ejb-adaptor** as the type of plug-in. Specify **127.0.0.1** as the hostname of the machine on which you installed the NIC host that supports the agent. Specify **1099** as the port number on which the name server runs.

   Specify **EJBObjectClustering** as the load-balancing scheme of the J2EE application server that hosts the SRC-VTA. Specify **vta-Jwo/SAEEventListenerBean** as the Java Naming and Directory Interface (JNDI) name of the SAEEventListener EJB of the peer SRC-VTA. Specify **org.jnp.interfaces.NamingContextFactory** as the class name of the J2EE application server's JNDI service provider.

```
[edit]
root@mob-src-63> set shared sae group POP-ID configuration plug-ins name vta
  ejb-adaptor application-server-url 127.0.0.1:1099
root@mob-src-63> set shared sae group POP-ID configuration plug-ins name vta
  ejb-adaptor ejb-clustering-strategy EJBObjectClustering
root@mob-src-63> set shared sae group POP-ID configuration plug-ins name vta
  ejb-adaptor jndi-sae-event-listener vta-Jwo/SAEEventListenerBean
root@mob-src-63> set shared sae group POP-ID configuration plug-ins name vta
  ejb-adaptor jndi-service-provider org.jnp.interfaces.NamingContextFactory
```

Configuring the C3000 Controller to Send LDAP Queries to the SBR

Step-by-Step Procedure

In this procedure you configure the C3000 Controller to send LDAP queries to the Steel-Belted Radius server. A Steel-Belted Radius server can authenticate against records stored in an external LDAP database.

1. Configure the controller to send LDAP queries to the SBR server. Paste the contents shown in the script file.

```
[edit]
root@mob-src-63> set shared sae group POP-ID subscriber-classifier rule script
  script
'# test by: java -cp /opt/UMC/sae/lib/sae.jar -jar /opt/UMC/sae/lib/jython.jar
 jysearch.py



from javax.naming import *
from java.util import *
from javax.naming.directory import *
myEnv = Hashtable()
myEnv.put(Context.INITIAL_CONTEXT_FACTORY,"com.sun.jndi.ldap.LdapCtxFactory")
myEnv.put(Context.PROVIDER_URL, "ldap://10.14.1.2:667/")
myEnv.put(Context.SECURITY_PRINCIPAL, "cn=admin,o=radius")
myEnv.put(Context.SECURITY_CREDENTIALS, "radius")
mySearch = SearchControls()
mySearch.setSearchScope(SearchControls.SUBTREE_SCOPE)
myAttBundle = "generic1"
myAttUName = "fullname"
myFilter = myAttBundle + "=*"
def getSbrSession(ucc):
  ctx = InitialDirContext(myEnv)
  myBase = "calling-station-id=" + ucc.macAddress.replace(\':\',\'-\') +
",radiusstatus=sessions_by_calling_station,o=radius"
  results = ctx.search(myBase,myFilter,mySearch)
  for rs in results:
    myBundle = rs.attributes.get(myAttBundle).get()
    myUserId = rs.attributes.get(myAttUName).get()
    if( ( len(myBundle) > 0 ) and ( len(myUserId) > 0 ) ):
      ctx.close()
      return "retailerName=default,o=users,o=umc?loginName=" + myUserId +
"?sub?(uniqueId=" + myBundle + ")"
  myBase = "user=" + ucc.macAddress +
",radiusstatus=sessions_by_user,o=radius"
  results = ctx.search(myBase,myFilter,mySearch)
  for rs in results:
    myBundle = rs.attributes.get(myAttBundle).get()
    if( len(myBundle) > 0 ):
```

```
      ctx.close()
      return "uniqueId=" + myBundle +
",ou=local,retailerName=default,o=users,o=UMC"
  ctx.close()
  return
classify.append(getSbrSession)
';
```

2. Create a JSRC policy list.

   Policy groups hold policy lists.

   Specify **JWO-P1** as the folder name, **SecureAccess-Policy** as the group name, and **PR** as the list name.

   Specify **both** to configure the applicability as ingress and egress interfaces. Specify **junos-ise** to configure the policy role for MX Series routers.

   ```
   [edit]
   root@mob-src-63> set policies folder JWO-P1 group SecureAccess-Policy list PR
     applicability both
   root@mob-src-63> set policies folder JWO-P1 group SecureAccess-Policy list PR
     role junos-ise
   ```

3. Create a JSRC policy rule that installs existing dynamic profiles.

   Specify **CR** as the name of the rule. Specify **Secure-EAP** as the name of the dynamic profile.

   ```
   [edit]
   root@mob-src-63> set policies folder JWO-P1 group SecureAccess-Policy list PR
     rule CR accounting
   root@mob-src-63> set policies folder JWO-P1 group SecureAccess-Policy list PR
     rule CR type junos-ise
   root@mob-src-63> set policies folder JWO-P1 group SecureAccess-Policy list PR
     rule CR dynamic-profile profile-name Secure-EAP
   ```

4. Add services to a global services scope.

   Specify **SecureSrv** as the name of the global service.

   Configure the time between interim accounting messages. Specify **60** seconds.

   ```
   [edit]
   root@mob-src-63> set services global service SecureSrv accounting-interim-interval
     60
   root@mob-src-63> set services global service SecureSrv available
   root@mob-src-63> set services global service SecureSrv policy-group
     /JWO-P1/SecureAccess-Policy
   root@mob-src-63> set services global service SecureSrv status active
   root@mob-src-63> set services global service SecureSrv tracking-plug-in vta
   root@mob-src-63> set services global service SecureSrv type normal
   ```

5. Configure the time between interim accounting messages for the **InternetSrv** service.

   Specify **600** seconds.

   ```
   [edit]
   root@mob-src-63> set services global service InternetSrv accounting-interim-interval
     600
   ```

Adding a Native User to the SBR Server

Step-by-Step Procedure

In this procedure you add native users to the SBR server using the SBR Administrator (GUI) for testing purposes. In your network, the server typically relies on another database to confirm the user's password.

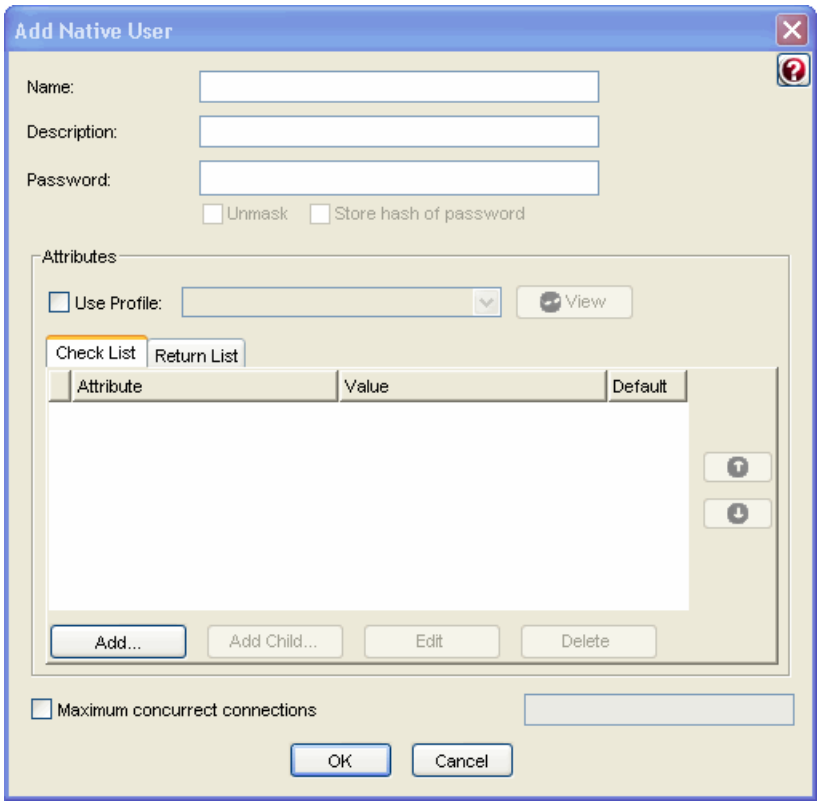
1. In the SBR Administrator window, select **Users > Native** in the sidebar.

   The Native Users panel appears.

2. Add a native user and click **Add**.

   The Add Native User dialog box appears as shown in Figure 5 on page 41.

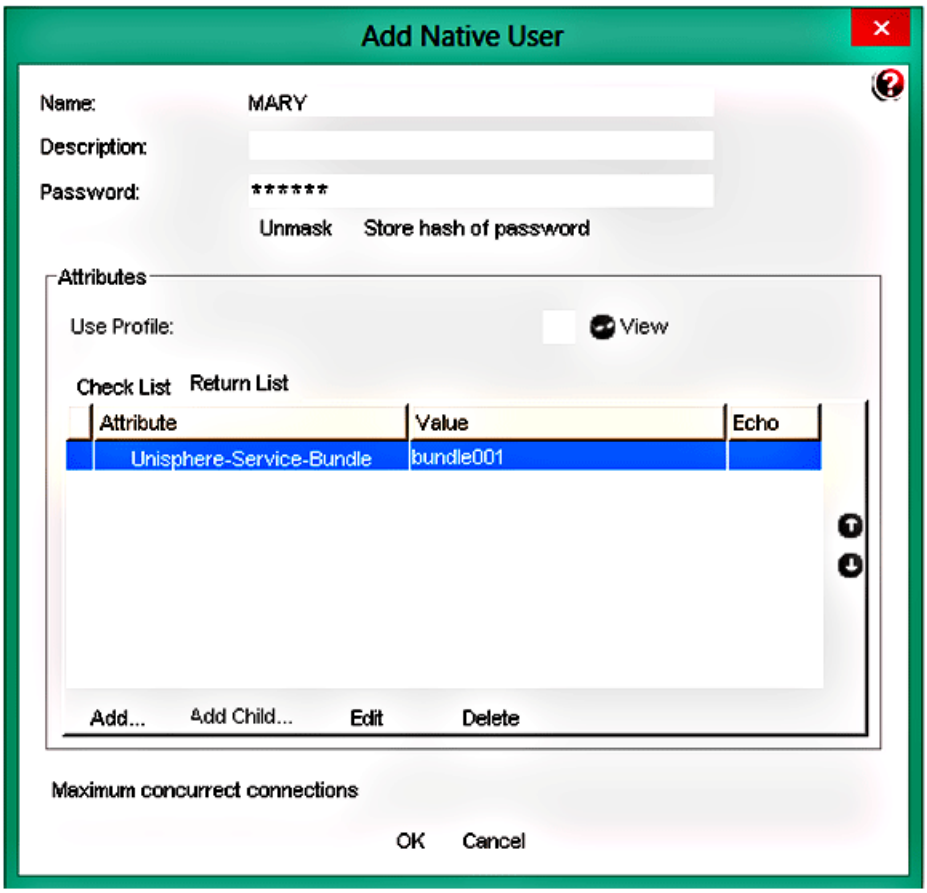
Figure 5: Add Native User Dialog Box



3. Enter the user's login name in the **Name** field, enter the password in the **Password** field, then click **OK**.

   In this example we add the user named **MARY** as shown in Figure 6 on page 42.

Figure 6: Native Users with Service Bundle Attribute

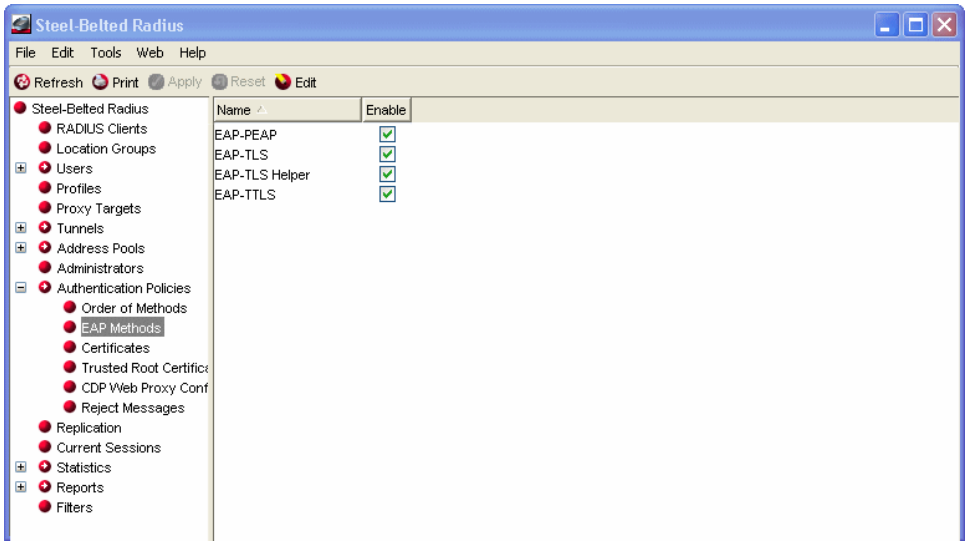


4. Enable the EAP authentication method.

   Select **Authentication Policies >EAP Methods**.

   Click the **Enable** check box to enable the EAP-PEAP authentication method. then click **Apply**.

Figure 7: Steel-Belted Radius Window

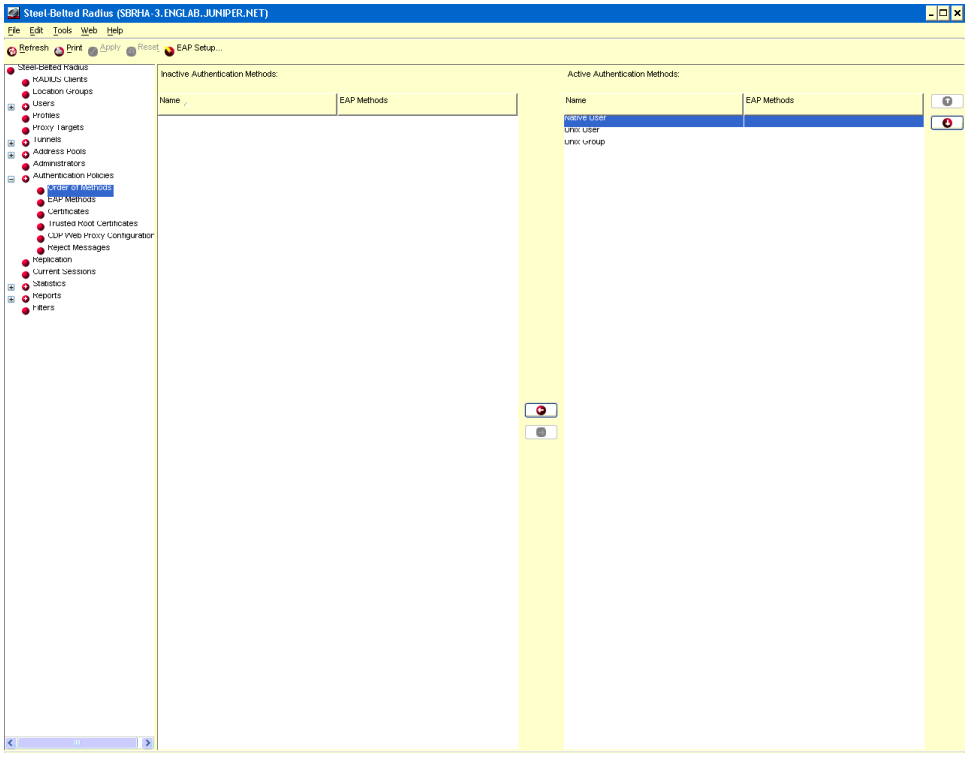


5. Activate and add an EAP-SIM method to the authentication policy.

   Select **Authentication Policies> Order of Methods**.

   The Active Authentication Methods panel appears as shown in Figure 8 on page 43.

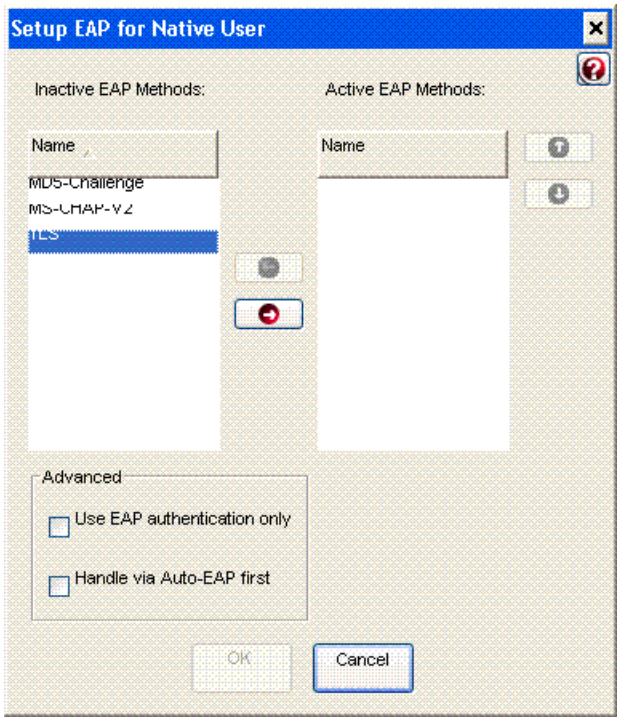
Figure 8: Active Authentication Methods Panel



6. Double-click the **Native User** authentication policy under the Name column and click **EAP Setup**.

The Setup EAP dialog is displayed as shown in Figure 9 on page 44.

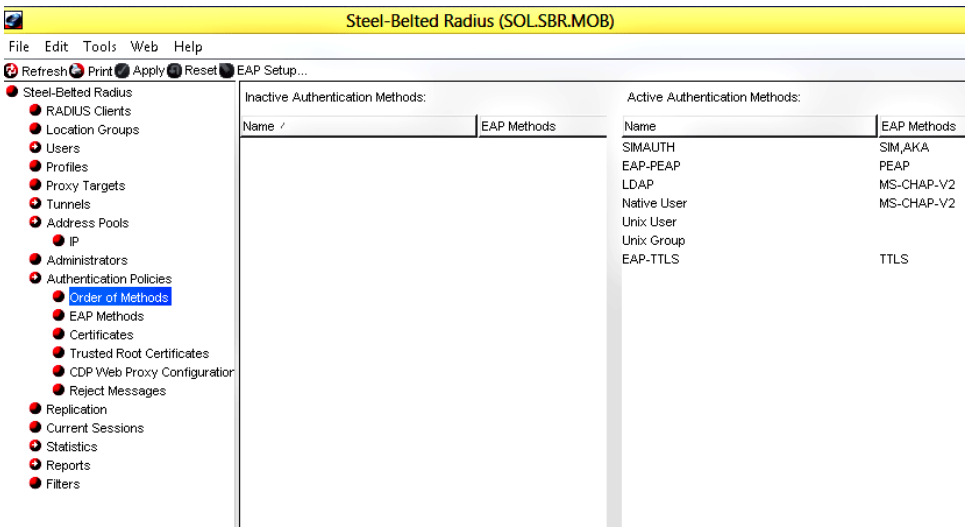
Figure 9: Setup EAP for Native User Window



7. Highlight the EAP-PEAP method, and click the right arrow button to move the method to the Active EAP Method column, then click **OK**.

8. Verify that the EAP methods are listed in the order you configured under the EAP Methods column for the selected authentication policy.

Figure 10: Active Authentication Methods Panel



Verification

Confirm that the configuration is working properly.

- Verifying the Redirect Profile for the Open Access Scenario on page 45
- Verifying the Subscriber Session on the C3000 Controller for the Open Access Scenario on page 46
- Verifying the Subscriber on the MX Series Router for the Secure Access Scenario on page 49
- Verifying the Subscriber Session on the C3000 Controller for the Secure Access Scenario on page 50

Verifying the Redirect Profile for the Open Access Scenario

Purpose After a test user connects to the Internet using the open access method, verify the redirect profile operation.

Action From operational mode on the MX Series router, run the **show subscribers** and **show subscribers extensive** commands.

```
sea-mobility@sol-mob-54> show subscribers

Interface           IP Address/VLAN ID                  User Name                       LS:RI
demux0.1073741830   10.2.1.13                                                   default:default
```

Verify that the demux interface is listed.

```
sea-mobility@sol-mob-54> show subscribers extensive
Type: DHCP
IP Address: 10.2.1.13
IP Netmask: 255.255.255.255
Logical System: default
Routing Instance: default
Interface: demux0.1073741830
Interface type: Dynamic
Dynamic Profile Name: demux-default-open-access
MAC Address: c0:9f:42:ed:01:ab
State: Active
Radius Accounting ID: 168
Session ID: 168
VLAN Id: 100
Login Time: 2012-10-15 14:13:45 EDT
Service Sessions: 1
DHCP Options: len 30
35 01 01 37 06 01 03 06 0f 77 fc 39 02 05 dc 3d 07 01 c0 9f
42 ed 01 ab 33 04 00 76 a7 00
IP Address Pool: Open-Dhcp-Pool

   Service Session ID: 172
   Service Session Name: Open-Portal
   State: Active
   IPv4 Input Filter Name: myifd-xe-4/2/0.100-demux0.1073741830-in
```

Meaning Verify the following:

- **Routing Instance:**—Check that the **default** routing instance is shown. If your network uses multiple instances, verify that the instance shown is the correct instance for the subscriber session being tested.
- **Session ID:**—Note the session identifier. The session identifier is useful for configuring billing and for troubleshooting.
- **Service Sessions:**—Check that **1** is shown as the number of service sessions. If the subscriber is using multiple services, verify that the number displayed matches the number of services under test.
- **Service Session Name:**—Check that the **Open-Portal** session is shown. The session name should match the session profile name you created. This verifies that the demux interface is created and a policy is applied.
- **IPv4 Input Filter Name:**—Check that the **myifd-xe-4/2/0.100-demux0.1073741830-in** interface and demux interface is shown. The input filter name should match the firewall filter name you created for the open access scenario.

If the Service Session Name and IPv4 Input Filter Name are correct, it indicates that the open scenario is working correctly.

Verifying the Subscriber Session on the C3000 Controller for the Open Access Scenario

Purpose After a user connects to the Internet using the open access method, verify the service activation engine subscriber information.

Action From operational mode on the C3000 Controller, run the **show sae subscribers terse** and **show sae subscribers** commands.

```
root@mob-src-63> show sae subscribers terse
User Sessions
Session ID                Login Name    IP Address
5VPddhOlXbZmwACj          BOB           10.2.1.13
```

Verify that the user login name being tested is displayed.

```
root@mob-src-63> show sae subscribers
User Session
User IPv4             10.2.1.13/32
User IPv6
Other IP Addresses    []
User DN          uniqueId=BOB,ou=local,retailername=default,o=Users,o=UMC
MAC Address           c0:9f:42:ed:01:ab
Device Name           default@sol-mob-54
Domain Name
Interface Name     demux0.1073741830
Interface Alias
Interface Description
Interface Type        IP
User Name             BOB
Primary User Name
Login Name       BOB
User Type             DIAMETER
Login Type       PORTAL
NAS Port ID           xe-4/2/0.100:100
NAS Port              1073741924
NAS IP                0.0.0.0
Session Substitutions []
Service Bundle
Calling Station Id
VPN Id
Session Properties    []
Relay Agent address   0.0.0.0
RADIUS session ID     5VPddhOlXbZmwACj
Login time            Mon Oct 15 14:14:20 EDT 2012
Session Timeout       -1

  User Profile
  User Dn          uniqueId=BOB,ou=local,retailername=default,o=Users,o=UMC
  Unauthenticated              false
  Current logins               1
  Logins with this user profile 1
  anonymous                    FALSE
  cn                           BOB
  sn                           Bob
  uniqueid                     BOB

    Subscription
    Subscription name InternetSrv
    activationorder   10000
    servicename     InternetSrv

sspaction          ACTIVATE_ON_LOGIN
    sspstate           SUBSCRIBED

  User Profile
```

```
  User Dn                       ou=local,retailerName=default,o=Users,o=UMC
  Unauthenticated               false
  Current logins                1
  Logins with this user profile 0
  ou                            local

  User Profile
  User Dn                       retailerName=default,o=Users,o=UMC
  Unauthenticated               false
  Current logins                1
  Logins with this user profile 0
  domainname                    default
  ou                            default
  retailername                  default

  Service Session
  Subscription Name    InternetSrv
  Session Name            default
  Service name            InternetSrv
  Start time              Mon Oct 15 14:14:20 EDT 2012
  RADIUS session ID       InternetSrv:BOB:1350324860624:477
  Session Properties      {}
  Interim Time            -1
  Service Session Version 7
  Attributes Version      4
  Session Timeout         -1
  Session Tag
  Upstream Bandwidth      -1
  Downstream Bandwidth    -1

    Provisioning Set
    Policy group name policyGroupName=Internet-Policy,ou=JWO-P1,o=Policies,o=UMC
    Type              intelligentServiceEdge
    Version           1
                      {AAAbothPL<
>=[{ISEProvisioningId#14156404819618698O9/sol-mob-54@mob.jnpr.net;0;168;1350059938,
 [juniper-policy-definition code: 2022
    Provisioning Set  flags: VM vendorId: VID_JNPR value: juniper-template-name
code: 2023 flags: VM vendorId: VID_JNPR value: Internet juniper-policy-name code:

                      2021 flags: VM vendorId: VID_JNPR value:
14156404819618698O9]}]}
```

Meaning Verify the following:

- **User Dn**—Check that **uniqueId=BOB,ou=local,retailername=default,o=Users,o=UMC** is shown. The user distinguished name should be the name configured in the SSPortal local authentication roles and properties.
- **Login Name**—Check that **BOB** is shown.
- **Login Type**—Check that **PORTAL** is shown.
- **Interface Name**—Note the **demux0.1073741830** demux interface name. The demux interface name is useful information when troubleshooting.
- **Subscription name**—Check that **InternetSrv** is shown. The InternetSrv name is configured on the C3000 Controller when you add normal services to the global service scope.

- **Servicename**—Check that **InternetSrv** is shown. The InternetSrv name is configured on the C3000 Controller when you add normal services to the global service scope.
- **Policy group name policyGroupName=**—Check that **Internet-Policy,ou=JWO-P1,o=Policies,o=UMC** is shown. This verifies that the policy is pushed to the router.

Verifying the Subscriber on the MX Series Router for the Secure Access Scenario

Purpose After a user connects to the Internet using the secure access method, verify the operation.

Action From operational mode on the MX Series router, run the **show subscribers extensive address 10.2.2.12** command.

```
sea-mobility@sol-mob-54> show subscribers extensive address 10.2.2.12
Type: DHCP
IP Address: 10.2.2.12
IP Netmask: 255.255.255.255
Logical System: default
Routing Instance: default
Interface: demux0.1073741831
Interface type: Dynamic
Dynamic Profile Name: demux-default
MAC Address: c0:9f:42:ed:01:ab
State: Active
Radius Accounting ID: 174
Session ID: 174
VLAN Id: 200
Login Time: 2012-10-15 16:17:21 EDT
Service Sessions: 1
DHCP Options: len 30
35 01 01 37 06 01 03 06 0f 77 fc 39 02 05 dc 3d 07 01 c0 9f
42 ed 01 ab 33 04 00 76 a7 00
IP Address Pool: Secure-Dhcp-Pool

    Service Session ID: 175
    Service Session Name: Secure-EAP
    State: Active
    IPv4 Input Filter Name: jwo-int-demux0.1073741831-in
```

Meaning Verify the following:

- **Interface:**—Note the **demux0.1073741830** demux interface name. The demux interface name is useful information when troubleshooting.
- **Session ID:**—Note the session identifier. The session identifier is useful for configuring billing and for troubleshooting.
- **Service Sessions:**—Check that **1** session is shown as the number of service sessions. If the subscriber is using multiple services, verify that the number displayed matches the number of services under test.
- **Service Session ID:**—Note the service session identifier. The session identifier is useful for configuring billing and for troubleshooting.

- **Service Session Name:**—Check that the **Secure-EAP** session is shown. The session name should match the session profile name you created. This verifies that a demux interface is created and a policy is applied.
- **IPv4 Input Filter Name:**—Check that the **jwo-int-demux0.1073741831-in** demux interface is shown. The input filter name should match the firewall filter name you created for the for secure access scenario.

  If the Interface, Service Session Name, and IPv4 Input Filter Name are correct, it indicates correct operation.

Verifying the Subscriber Session on the C3000 Controller for the Secure Access Scenario

Purpose After a user connects to the Internet using the secure access method, verify the operation.

Action From operational mode on the C3000 Controller, run the **show sae subscribers terse** and **show sae subscribers ip address 10.2.2.12** commands.

```
root@mob-src-63> show sae subscribers terse
User Sessions
Session ID                Login Name     IP Address
5VPddhOlXbZmwACm          MARY           10.2.2.12
```

Verify that the user login name being tested is displayed.

```
root@mob-src-63> show sae subscribers ip address 10.2.2.12
User Session
User IPv4             10.2.2.12/32
User IPv6
Other IP Addresses    []
User DN       uniqueId=bundle001,ou=local,retailerName=default,o=users,o=umc
MAC Address           c0:9f:42:ed:01:ab
Device Name           default@sol-mob-54
Domain Name
Interface Name    demux0.1073741831
Interface Alias
Interface Description
Interface Type        IP
User Name      MARY
Primary User Name
Login Name            MARY
User Type             DIAMETER
Login Type            ADDR
NAS Port ID           xe-4/2/0.200:200
NAS Port              1073742024
NAS IP                0.0.0.0
Session Substitutions []
Service Bundle
Calling Station Id
VPN Id
Session Properties    []
Relay Agent address   0.0.0.0
RADIUS session ID     5VPddhOlXbZmwACm
Login time            Mon Oct 15 16:17:22 EDT 2012
Session Timeout       -1

  User Profile
  User Dn         uniqueId=bundle001,ou=local,retailerName=default,o=users,o=umc
  Unauthenticated               false
  Current logins                1
  Logins with this user profile 0
  anonymous                     FALSE
  cn                            EAP-Bundle
  loginname                     MARY
  sn                            EAP-Bundle
  uniqueid                      bundle001

    Subscription
    Subscription name SecureSrv
    activationorder   10000
    servicename       SecureSrv
    sspaction         ACTIVATE_ON_LOGIN
    sspstate          SUBSCRIBED

  User Profile
```

```
  User Dn                       ou=local,retailerName=default,o=Users,o=UMC
  Unauthenticated               false
  Current logins                2
  Logins with this user profile 0
  ou                            local

  User Profile
  User Dn                       retailerName=default,o=Users,o=UMC
  Unauthenticated               false
  Current logins                2
  Logins with this user profile 0
  domainname                    default
  ou                            default
  retailername                  default

  Service Session
  Subscription Name    SecureSrv
  Session Name             default
  Service name      SecureSrv
  Start time               Mon Oct 15 16:17:22 EDT 2012
  RADIUS session ID        SecureSrv:MARY:1350332242742:486
  Session Properties       {}
Interim Time             -1
  Service Session Version 7
  Attributes Version       4
  Session Timeout          -1
  Session Tag
  Upstream Bandwidth       -1
  Downstream Bandwidth     -1

    Provisioning Set
    Policy group name policyGroupName=SecureAccess-Policy,ou=JWO-P1,o=Policies,o=UMC

    Type               intelligentServiceEdge
    Version            1
                       {AAAbothPL<
>=[{ISEProvisioningId#14156404819618698l9/sol-mob-54@mob.jnpr.net;0;174;1350059938,
 [juniper-policy-definition code: 2022
    Provisioning Set  flags: VM vendorId: VID_JNPR value: juniper-template-name
code: 2023 flags: VM vendorId: VID_JNPR value: Secure-EAP juniper-policy-name
                       code: 2021 flags: VM vendorId: VID_JNPR value:
14156404819618698l9]}]}
```

Meaning Verify the following:

- **User Dn**—Check that the **uniqueId=bundle001,ou=local,retailerName=default,o=users,o=umc** user distinguished name is shown.
- **Interface Name**—Check that the **demux0.1073741831** interface is shown. The demux interface number should match the number displayed on the MX Series router in the previous verification steps.
- **User Name**—Check that **MARY** is shown.
- **Subscription Name**—Check that **SecureSrv** is shown. The InternetSrv name is configured on the C3000 Controller when you add normal services to the global service scope.

Related Documentation

- Service Provider Wi-Fi Drivers on page 5
- Service Provider Wi-Fi Services Supporting Open and Secure Access on page 7