

## Configuring Access Profiles for L2TP or PPP Parameters (NSM Procedure)

---

You can set up access profiles to validate Layer 2 Tunneling Protocol (L2TP) connections and session requests. You can configure multiple profiles. You can also configure multiple clients for each profile. See the following topics:

1. Configuring Access Profile (NSM Procedure) on page 1
2. Configuring Accounting Parameters for Access Profiles (NSM Procedure) on page 2
3. Configuring the Accounting Order (NSM Procedure) on page 2
4. Configuring the Authentication Order (NSM Procedure) on page 3
5. Configuring the Authorization Order (NSM Procedure) on page 4
6. Configuring the L2TP Client (NSM Procedure) on page 4
7. Configuring the Client Filter Name (NSM Procedure) on page 5
8. Configuring the LDAP Options (NSM Procedure) on page 6
9. Configuring the LDAP Server (NSM Procedure) on page 7
10. Configuring the Provisioning Order (NSM Procedure) on page 8
11. Configuring RADIUS Parameters for AAA Subscriber Management (NSM Procedure) on page 9
12. Configuring the RADIUS Parameters (NSM Procedure) on page 11
13. Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure) on page 12
14. Configuring Session Limit (NSM Procedure) on page 13

### Configuring Access Profile (NSM Procedure)

To configure an access profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 1.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 1: Access Profile Properties Configuration Details**

Task	Your Action
Configure access profile properties.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Profile.</li> <li>2. In the <b>Name</b> box, enter the name of the profile.</li> <li>3. In the <b>Comment</b> box, enter the comment.</li> </ol>

### **Configuring Accounting Parameters for Access Profiles (NSM Procedure)**

To configure RADIUS accounting parameters for an access profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 2.
6. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 2: Accounting Parameter Configuration Details**

Task	Your Action
Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Profile.</li> <li>2. Click <b>Accounting</b> next to profile.</li> <li>3. In the <b>Comment</b> box, enter the comment.</li> <li>4. Select the <b>Accounting Stop On Failure</b> check box to configure RADIUS accounting to send an Acct-Stop message when client access fails AAA but the AAA server grants access.</li> <li>5. Select the <b>Accounting Stop On Access Deny</b> check box to configure RADIUS accounting to send an Acct-Stop message when the AAA server denies a client access.</li> <li>6. Select the <b>Immediate Update</b> check box to configure the router to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message.</li> <li>7. From the <b>Update Interval</b> list, select the amount of time between updates, in minutes. Range: 10 through 1440 minutes Default: no updates</li> <li>8. From the <b>Statistics</b> list, select the time statistics for the sessions being managed by AAA.</li> </ol>

### **Configuring the Accounting Order (NSM Procedure)**

Beginning with JUNOS Release 8.0, you can configure RADIUS accounting for an Layer 2 Tunneling Protocol (L2TP) profile. With RADIUS accounting enabled, Juniper Networks routers, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands.

When you enable RADIUS accounting for an L2TP profile, it applies to all the clients within that profile. You must enable RADIUS accounting on at least one LT2P profile for the RADIUS authentication server to send accounting stop and start messages.

To configure accounting order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 3.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 3: Accounting Order Configuration Details**

Task	Your Action
Configure the accounting order.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Profile.</li><li>2. Click <b>Accounting Order</b> next to Profile.</li><li>3. Click <b>Add new entry</b> next to Accounting Order.</li><li>4. In the <b>New accounting-order</b> window, select <b>radius</b> to use RADIUS accounting method.</li></ol>

### **Configuring the Authentication Order (NSM Procedure)**

You can configure the order in which the JUNOS Software tries different authentication methods when authenticating peers. For each access attempt, the software tries the authentication methods in order, from first to last.

To configure authentication order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 4.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 4: Authentication Order Configuration Details**

Task	Your Action
Configure the authentication order.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Profile.</li><li>2. Click <b>Authentication Order</b> next to Profile.</li><li>3. Click <b>Add new entry</b> next to Accounting Order.</li><li>4. In the <b>New authentication-order</b> window, select the order in which the JUNOS Software tries different authentication methods when verifying that a client can access the router.</li></ol>

### **Configuring the Authorization Order (NSM Procedure)**

To configure authorization order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 5.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 5: Authorization Order Configuration Details**

Task	Your Action
Configure the authorization order.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Profile.</li><li>2. Click <b>Authorization Order</b> next to Profile.</li><li>3. Click <b>Add new entry</b> next to Authorization Order.</li><li>4. In the <b>New authorization-order</b> window, select the authorization order.</li></ol>

### **Configuring the L2TP Client (NSM Procedure)**

To configure the Layer 2 Tunneling Protocol (L2TP) Client in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 6.
6. Click one:
  - OK—Saves the changes.

- Cancel—Cancels the modifications.

**Table 6: Client Configuration Details**

Task	Your Action
Configure the client.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Profile.</li> <li>2. Click <b>Client</b> next to Profile.</li> <li>3. Click <b>Add new entry</b> next to Client.</li> <li>4. In the <b>Name</b> box, enter the client name.</li> <li>5. In the <b>Comment</b> box, enter the comment.</li> <li>6. In the <b>Chap Secret</b> box, enter the secret key associated with a peer.</li> <li>7. In the <b>pap password</b> box, enter the Password Authentication Protocol (PAP) password.</li> </ol>
Configure a client group.	<ol style="list-style-type: none"> <li>1. Click <b>Client Group</b> next to client.</li> <li>2. Click <b>Add new entry</b> next to Client Group.</li> <li>3. In the <b>New client-group</b> window, enter the client group.</li> </ol>
Configure a firewall user.	<ol style="list-style-type: none"> <li>1. Click <b>Firewall User</b> next to client.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. In the <b>Password</b> box, enter the password.</li> </ol>
Configure PPP properties for a client profile.	<ol style="list-style-type: none"> <li>1. Click <b>Ppp</b> next to client.</li> <li>2. Select <b>ike</b> to configure an IKE access profile. <ol style="list-style-type: none"> <li>a. In the <b>Comment</b> box, enter the comment.</li> <li>b. Select <b>Initiate Dead Peer Detection</b> to detect inactive peers on dynamic IPsec tunnels.</li> <li>c. In the <b>Interface Id</b> box, enter the interface identifier.</li> <li>d. Click <b>Allowed Proxy Pair</b> next to Ike.</li> <li>e. Click <b>Add new entry</b> next to Allowed Proxy Pair.</li> <li>f. In the <b>Local</b> box, enter the network address of the local peer.</li> <li>g. In the <b>Remote</b> box, enter the network address of the remote peer.</li> <li>h. In the <b>Comment</b> box, enter the comment.</li> <li>i. Click <b>Pre Shared Key</b> next to Ike. <ol style="list-style-type: none"> <li>a. Select <b>pre-shared-key</b> to configure the key used to authenticate a dynamic peer during IKE phase 1 negotiation and select the key.</li> <li>b. In the <b>Comment</b> box, enter the comment.</li> <li>c. Click <b>Ascii Text</b> next to Pre Shared key.</li> <li>d. In the <b>ascii-text</b> box, enter the string.</li> <li>e. Select <b>Ike-policy</b> to authenticate dynamic peers during IKE negotiation and select the policy name.</li> </ol> </li> </ol> </li> </ol>

### **Configuring the Client Filter Name (NSM Procedure)**

To configure restrictions on client names in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.

3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 10.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 7: Client Filter Name Configuration Details**

Task	Your Action
Configure the restrictions on client names.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Profile.</li> <li>2. Click <b>Client Name Filter</b> next to profile.</li> <li>3. In the <b>Comment</b> box, enter the comment.</li> <li>4. In the <b>Domain Name</b> box, enter the domain name.</li> <li>5. In the <b>Separator</b> box, enter the separator character in domain name.</li> <li>6. From the <b>Count</b> list, select the number of separator instances. Range: 0 through 255</li> </ol>

### **Configuring the LDAP Options (NSM Procedure)**

To configure Lightweight Directory Access Protocol (LDAP) options in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 8.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 8: Ldap Options Configuration Details**

Task	Your Action
Configure lightweight directory access protocol options.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Profile.</li> <li>2. Click <b>Ldap Options</b> next to profile.</li> <li>3. In the <b>Comment</b> box, enter the comment.</li> <li>4. From the <b>Revert Interval</b> list, select the amount of time the router waits after a server has become unreachable. Range: 60 through 4294967295 Default: 600</li> <li>5. In the <b>Base Distinguished Name</b> box, enter the suffix when assembling user distinguished name (DN) or base DN under which to search for user DN.</li> </ol>
Derive user distinguished name from common-name and base-distinguished-name.	<ol style="list-style-type: none"> <li>1. Click <b>Assemble</b> next to Ldap Options.</li> <li>2. Select one of the following: <ul style="list-style-type: none"> <li>■ <b>assemble</b>—To derive user distinguished name from common-name and base-distinguished-name. <ol style="list-style-type: none"> <li>a. In the <b>Comment</b> box, enter the comment.</li> <li>b. In the <b>Common Name</b> box, enter the common name.</li> </ol> </li> <li>■ <b>search</b>—To search for user's distinguished name. <ol style="list-style-type: none"> <li>a. In the <b>Comment</b> box, enter the comment.</li> <li>b. In the <b>Search Filter</b> box, enter the filter to use in search.</li> <li>c. Click <b>Admin Search</b> next to Search.</li> <li>d. In the <b>Comment</b> box, enter the comment.</li> <li>e. In the <b>Distinguished Name</b> box, enter the user distinguished name.</li> <li>f. In the <b>Password</b> box, enter the password.</li> </ol> </li> </ul> </li> </ol>

### Configuring the LDAP Server (NSM Procedure)

To configure Lightweight Directory Access Protocol (LDAP) server in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 9.
6. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 9: Ldap Server Configuration Details**

Task	Your Action
Configure LDAP server.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Profile.</li> <li>2. Click <b>Ldap Server</b> next to profile.</li> <li>3. Click <b>Add new entry</b> next to Ldap Server.</li> <li>4. In the <b>Name</b> box, enter the name of the server.</li> <li>5. In the <b>Comment</b> box, enter the comment.</li> <li>6. From the <b>Port</b> list, select the port number on which to contact the RADIUS server (LDAP server)</li> <li>7. In the <b>Source Address</b> box, enter a valid IPv4 address configured on one of the router interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.</li> <li>8. From the <b>Routing Instances</b> list, select the routing instance name.</li> <li>9. From the <b>Retry</b> list, select the number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 10 Default: 3</li> <li>10. From the <b>Timeout</b> list, select the amount of time that the local router waits to receive a response from a RADIUS server. Range: 3 through 90 Default: 5</li> </ol>

### Configuring the Provisioning Order (NSM Procedure)

To configure the provisioning order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 10.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 10: Provisioning Order Configuration Details**

Task	Your Action
Configure the provisioning order.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Profile.</li> <li>2. Click <b>Provisioning Order</b> next to profile.</li> <li>3. Click <b>Add new entry</b> next to Provisioning Order.</li> <li>4. In the <b>New provisioning-order</b> window, select the order in which provisioning mechanisms are used.</li> </ol>

## Configuring RADIUS Parameters for AAA Subscriber Management (NSM Procedure)

You can specify the RADIUS parameters for the subscriber access manager feature. You can specify the IP addresses of the RADIUS servers used for authentication and accounting, options that provide configuration information for the RADIUS servers, and how RADIUS attributes are used.

To configure radius parameters for AAA subscriber management in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 11.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 11: Radius Parameter Configuration Details**

<b>Task</b>	<b>Your Action</b>
Configure the RADIUS parameters.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Profile.</li><li>2. Click <b>Radius</b> next to Profile.</li><li>3. In the <b>Comment</b> box, enter the comment.</li></ol>
Specify a list of the RADIUS accounting servers used for accounting for Dynamic Host Configuration Protocol (DHCP), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Protocol (PPP) clients.	<ol style="list-style-type: none"><li>1. Click <b>Attributes</b> next to Radius.</li><li>2. In the <b>Comment</b> box, enter the comment.</li></ol>

**Table 11: Radius Parameter Configuration Details** (continued)

Task	Your Action
Configure the router to exclude the specified attributes from the specified type of RADIUS message.	<ol style="list-style-type: none"> <li>1. Click <b>Exclude</b> next to Radius.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. From the listed RADIUS attribute type, select the attributes to be excluded. RADIUS attribute types are: <ul style="list-style-type: none"> <li>■ <b>accounting-authentic</b>—RADIUS attribute 45, Acct-Authentic</li> <li>■ <b>accounting-delay-time</b>—RADIUS attribute 41, Acct-Delay-Time</li> <li>■ <b>accounting-session-id</b>—RADIUS attribute 44, Acct-Session-Id</li> <li>■ <b>accounting-terminate-cause</b>—RADIUS attribute 49, Acct-Terminate-Cause</li> <li>■ <b>called-station-id</b>—RADIUS attribute 30, Called-Station-Id</li> <li>■ <b>calling-station-id</b>—RADIUS attribute 31, Calling-Station-Id</li> <li>■ <b>class</b>—RADIUS attribute 25, Class</li> <li>■ <b>dhcp-gi-address</b>—Juniper VSA 26-57, DHCP-GI-Address</li> <li>■ <b>dhcp-mac-address</b>—Juniper VSA 26-56, DHCP-MAC-Address</li> <li>■ <b>Dhcp Options</b>— Excludes RADIUS attribute 26-55</li> <li>■ <b>event-timestamp</b>—RADIUS attribute 55, Event-Timestamp</li> <li>■ <b>framed-ip-address</b>—RADIUS attribute 8, Framed-IP-Address</li> <li>■ <b>framed-ip-netmask</b>—RADIUS attribute 9, Framed-IP-Netmask</li> <li>■ <b>input-filter</b>—Juniper VSA 26-10, Ingress-Policy-Name</li> <li>■ <b>input-gigapackets</b>—Juniper VSA 26-42, Acct-Input-Gigapackets</li> <li>■ <b>input-gigawords</b>—RADIUS attribute 52, Acct-Input-Gigawords</li> <li>■ <b>interface-description</b>—Juniper VSA 26-53, Interface-Desc</li> <li>■ <b>nas-identifier</b>—RADIUS attribute 32, NAS-Identifier</li> <li>■ <b>nas-port</b>—RADIUS attribute 5, NAS-Port</li> <li>■ <b>nas-port-id</b>—RADIUS attribute 87, NAS-Port-Id.</li> <li>■ <b>nas-port-type</b>—RADIUS attribute 61, NAS-Port-Type</li> <li>■ <b>output-filter</b>—Juniper VSA 26-11, Egress-Policy-Name</li> <li>■ <b>output-gigapackets</b>—Juniper VSA 25-43, Acct-Output-Gigapackets</li> <li>■ <b>output-gigawords</b>—RADIUS attribute 53, Acct-Output-Gigawords</li> </ul> </li> </ol>
Configure the router to ignore the specified attributes in RADIUS Access-Accept messages.	<ol style="list-style-type: none"> <li>1. Click <b>Ignore</b> next to client.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. Select the following check boxes to ignore the specified attributes: <ul style="list-style-type: none"> <li>■ <b>output-filter</b>—Egress-Policy-Name (VSA 26-11)</li> <li>■ <b>input-filter</b>—Ingress-Policy-Name (VSA 26-10)</li> <li>■ <b>framed-ip-netmask</b>—Framed-IP-Netmask (RADIUS attribute 9)</li> <li>■ <b>logical-system-routing-instance</b>—Virtual-Router (VSA 26-1)</li> </ul> </li> </ol>
Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients.	<ol style="list-style-type: none"> <li>1. Click <b>Authentication Server</b> next to Radius.</li> <li>2. Click <b>Add new entry</b> next to Authentication Server.</li> <li>3. In the <b>New authentication-server</b> window, enter the IPv4 address.</li> </ol>

**Table 11: Radius Parameter Configuration Details (continued)**

Task	Your Action
Configure the options used by RADIUS authentication and accounting servers.	<ol style="list-style-type: none"> <li>1. Click <b>Options</b> next to Radius.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. Select the <b>Ethernet Port Type Virtual</b> check box to specify a port type of virtual.</li> <li>4. From the <b>Interface Description Format</b> list, select the information that is included in or omitted from the interface description that the router passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). Select one of the following: <ul style="list-style-type: none"> <li>■ <b>sub-interface</b>—To specify the subinterface.</li> <li>■ <b>adapter</b>—To specify the adapter.</li> </ul> </li> <li>5. In the <b>Nas Identifier</b> box, enter a string in the range from 1 to 64 characters.</li> <li>6. From the <b>Accounting Session Id Format</b> list, select the format the router uses to identify the accounting session. Select one of the following: <ul style="list-style-type: none"> <li>■ <b>decimal</b>—To use the decimal format.</li> <li>■ <b>description</b>—To use the generic format, in the form jnpr interface-specifier:subscriber-session-id. Default: decimal</li> </ul> </li> <li>7. From the <b>Revert Interval</b> list, select the amount of time the router waits after a server has become unreachable. Range: 60 through 4294967295 seconds Default: 600 seconds</li> <li>8. Select the <b>vlan-nas-port-stacked-format</b> check box to configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.</li> </ol>
Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.	<ol style="list-style-type: none"> <li>1. Click <b>Nas Port Extended Format</b> next to Options.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. From the <b>Slot Width</b> list, select the number of bits in the slot field.</li> <li>4. From the <b>Adapter Width</b> list, select the number of bits in the adapter field.</li> <li>5. From the <b>Port Width</b> list, select the number of bits in the port field.</li> <li>6. From the <b>Stacked Vlan Width</b> list, select the number of bits in the SVLAN ID field.</li> <li>7. From the <b>Vlan Width</b> list, select the number of bits in the VLAN ID field.</li> </ol>

**Configuring the RADIUS Parameters (NSM Procedure)**

You can specify the options used by the RADIUS authentication and accounting servers.

To configure the radius parameters in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.

5. Add or modify settings as specified in Table 12.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.



**NOTE:** To create a profile, the device should be in the in-device policy mode.

---

**Table 12: Radius Parameters Configuration Details**

Task	Your Action
Configure the radius parameters.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Profile.</li> <li>2. Click <b>Radius Options</b> next to Profile.</li> <li>3. In the <b>Comment</b> box, enter the comment.</li> <li>4. From the <b>Revert Interval</b> list, select the amount of time the router waits after a server has become unreachable. Default: 600 seconds</li> </ol>

---

### **Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure)**

You can configure RADIUS for subscriber access management, L2TP, or PPP. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

To configure the radius server in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 13.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 13: Radius Server Configuration Details**

Task	Your Action
Configure the RADIUS servers.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Profile</li><li>2. Click <b>Radius Server</b> next to Profile.</li><li>3. In the <b>Name</b> box, enter the profile name.</li><li>4. In the <b>Comment</b> box, enter the comment.</li><li>5. From the <b>Port</b> list, select the port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865)</li><li>6. In the <b>Secret</b> box, enter the password to use with the RADIUS server. The secret password used by the local router must match that used by the server.</li><li>7. From the <b>Timeout</b> list, select the amount of time that the local router waits to receive a response from a RADIUS server. Range: 3 through 90 seconds Default: 3 seconds</li><li>8. From the <b>Retry</b> list, select the number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 10 Default: 3</li><li>9. In the <b>Source Address</b> box, enter a valid IPv4 address configured on one of the router interfaces.</li><li>10. From the <b>Routing Instance</b> list, select the routing instance name.</li></ol>

### **Configuring Session Limit (NSM Procedure)**

To configure the timeout limit in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 14.
6. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 14: Session Limit Configuration Details**

<b>Task</b>	<b>Your Action</b>
Configure the timeout interval.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Profile.</li><li>2. Click <b>Session Options</b> next to Profile.</li><li>3. In the <b>Comment</b> box, enter the comment.</li><li>4. From the <b>Client Idle Timeout</b> list, select the time in minutes of idleness after which access is denied. Range: 1 through 255 minutes</li><li>5. From the <b>Client Session Timeout</b> list, select the time in minutes since initial access after which access is denied.</li></ol>
Configure a client group.	<ol style="list-style-type: none"><li>1. Click <b>Client Group</b> next to Session Option.</li><li>2. Click <b>Add new entry</b> next to Client Group.</li><li>3. In the <b>New client-group</b> window, enter the client group.</li></ol>

Published: 2009-08-23