

Chapter 19

Configure System Authentication

You can configure the router to use RADIUS or TACACS+ authentication, or both, to validate users who attempt to access the router using Telnet. If you configure both authentication methods, you also can configure which method to try first.

For TACACS+ , the JUNOS software supports authentication, but does not support authorization.

When configuring system authentication, you can do the following:

- Configure RADIUS Authentication on page 199

- Configure TACACS+ Authentication on page 201

- Configure Shared User Accounts for RADIUS and TACACS+ Authentication on page 201

- Configure the Authentication Order on page 202

For an example of configuring system authentication, see “Examples: Configure System Authentication” on page 203.

Configure RADIUS Authentication

To use RADIUS authentication on the router, configure information about one or more RADIUS servers on the network by including the `radius-server` statement at the [edit system] hierarchy level:

```
[edit system]
radius-server server-address {
  port number;
  secret password;
  retry number;
  timeout seconds;
}
```

In *server-address*, specify the address of the RADIUS server.

You can specify a port number on which to contact the RADIUS server. By default, port number 1812 is used (as specified in RFC 2138).

You must specify a secret (password) that the local router passes to the RADIUS client (in the secret statement). Secrets can contain spaces. The secret used by the local router must match that used by the server.

Optionally, you can specify the amount of time that the local router waits to receive a response from a RADIUS server (in the timeout statement) and the number of times that the router attempts to contact a RADIUS authentication server (in the retry statement). By default, the router waits 3 seconds. You can configure this to be a value in the range 1 through 90 seconds. By default, the router retries connecting to the server 3 times. You can configure this to be a value in the range 1 through 10 times.

To configure multiple RADIUS servers, include multiple radius-server statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the user statement at the [edit system login] hierarchy level as described in “Configure Shared User Accounts for RADIUS and TACACS+ Authentication” on page 201.

Configure Juniper Networks–Specific RADIUS Attributes

The JUNOS software supports the configuration of Juniper Networks–specific RADIUS attributes. These attributes are known as vendor-specific attributes and are described in RFC 2138, *Remote Authentication Dial In User Service*. These Juniper Networks–specific attributes are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. Table 6 lists the Juniper Networks–specific attributes you can configure.

Table 6: Juniper Networks–Specific RADIUS Attributes

Name	Description	Type	Length	String
Juniper-Local-User-Name	Indicates the name of the user template used by this user when logging into a device. This attribute is used only in Access-Accept packets.	1	≥3	One or more octets containing printable ASCII characters.
Juniper-Allow-Commands	Contains an extended regular expression that allows the user to run commands in addition to the commands authorized by the user’s login class permission bits. This attribute is used only in Access-Accept packets.	2	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.
Juniper-Deny-Commands	Contains an extended regular expression that denies the user permission to run commands authorized by the user’s login class permission bits. This attribute is used only in Access-Accept packets.	3	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.

Configure TACACS+ Authentication

To use TACACS+ authentication on the router, configure information about one or more TACACS+ servers on the network by including the `tacplus-server` statement at the [edit system] hierarchy level:

```
[edit system]
tacplus-server server-address {
  secret password;
  single-connection;
  timeout seconds;
}
```

In `server-address`, specify the address of the TACACS+ server.

You must specify a secret (password) that the local router passes to the TACACS+ client (in the secret statement). Secrets can contain spaces. The secret used by the local router must match that used by the server.

You can optionally specify the amount of time that the local router waits to receive a response from a TACACS+ server (in the timeout statement) By default, the router waits 3 seconds. You can configure this to be a value in the range 1 through 90 seconds.

Optionally, you can have the software maintain one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt, thus optimizing attempts to connect to a TACACS+ server. To do this, include the `single-connection` statement.

To configure multiple TACACS+ servers, include multiple `tacplus-server` statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the user statement at the [edit system login] hierarchy level as described in “Configure Shared User Accounts for RADIUS and TACACS+ Authentication” on page 201.

Configure Shared User Accounts for RADIUS and TACACS+ Authentication

When you are using local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or TACACS+ authentication, you can create a shared user account that can be used by all users who do not have an individual account configured locally on the system. These accounts are sometimes called *template* accounts.

To enable a shared remote user account, create a user account with the user name “remote” and specify the privileges that you want to provide to these remote users:

```
[edit]
system {
  login {
    user remote {
      full-name "All remote users";
      uid uid-value;
      class class-name;
    }
  }
}
```

Privileges and file ownership are shared by all users who share the “remote” account. To specify exceptions to this account, but still use a remote authentication service, configure individual local accounts for those users.



Note

When you are using TACACS+ , the template account must have the user name “remote.” You cannot change the name of this account or configure other template accounts.

For information about creating user accounts, see “Configure User Accounts” on page 210. For an example of how to configure a shared account, see “Examples: Configure System Authentication” on page 203.

Configure the Authentication Order

If you configure the router to be both a RADIUS and TACACS+ client (by including the radius-server and tacplus-server statements), you can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying that a user can access the router. For each login attempt, the JUNOS software tries the authentication methods in order, starting with the first one, until the password matches.

To configure the authentication order, include the authentication-order statement at the [edit system] hierarchy level:

```
[edit system]
authentication-order [ authentication-methods ];
```

In *authentication-methods*, specify one or more of the following in the desired order, from first tried to last tried:

radius—Verify the user using RADIUS authentication services.

tacplus—Verify the user using TACACS+ authentication services.

password—Verify the user using the password configured for the user with the authentication statement at the [edit system login user] hierarchy level.

If you do not include the authentication-order statement, users are verified based on their configured password.

Examples: Configure System Authentication

Allow logins only by users who have been authenticated by a remote RADIUS server for the individual user Philip and for all other users validated by the RADIUS server. If Philip tries to log into the system, if the RADIUS server authenticates him, he is given access and privileges for the superuser class. Local accounts are not configured for the users Alexander and Darius. When they try to log into the system, if the RADIUS server authenticates them, they are given access with user ID (UID) 9999 and privileges for the operator class.

```
[edit]
system {
  login {
    authentication-order radius;
    user philip {
      full-name "Philip of Macedonia";
      uid 1001;
      class superuser;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class operator;
    }
  }
}
```

Configuring a single “remote” user template account requires that all users without individual configuration entries share the same class and UID. When you are using RADIUS and Telnet or RADIUS and SSH together, you can specify a different template user other than the “remote” user. This functionality is not available with TACACS+ . To configure an alternate template user, specify the “User-Name” parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample JUNOS configuration:

```
[edit]
system {
  login {
    user philip {
      full-name "Philip of Macedonia";
      uid 1001;
      class superuser;
    }
    user operator {
      full-name "All operators";
      uid 9990;
      class read-only;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}
```

Assume your RADIUS server is configured with the following information:

User Philip with password “olympia”

User Alexander with password “bucephalus” and user name “operator”

User Darius with password “redhead” and user name “operator”

User Roxane with password “alpo”

Philip would be given access as a superuser, because he has his own local user account. Alexander and Darius share UID 9990 and have access as an operator. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.



Note

When you are using TACACS+ , the template account must have the user name “remote.” You cannot change the name of this account or configure other template accounts.