

Chapter 28

Access Configuration Guidelines

To configure access, include statements at the [edit access] hierarchy level:

```
[edit access]
profile profile-name {
  authentication-order [ authentication-methods ];
  client name chap-secret data;
}
traceoptions {
  flag all;
  flag authentication;
  flag chap;
  flag configuration;
  flag radius;
}
```

This chapter discusses the following topics:

Configure Challenge Handshake Authentication Protocol on page 401

Configure the Authentication Order on page 403

Trace Access Processes on page 404

Summary of Access Configuration Statements on page 404

Configure Challenge Handshake Authentication Protocol

The Challenge Handshake Authentication Protocol (CHAP) allows each end of a PPP link to authenticate its peer, as defined in RFC 1994. The authenticator sends its peer a randomly generated challenge that the peer must encrypt using a one-way hash; the peer must then respond with that encrypted result. The key to the hash is a secret known only to the authenticator and authenticated. When the response is received, the authenticator compares its calculated result with the peer's response. If they match, the peer is authenticated.

Each end of the link identifies itself to its peer by including its name in the CHAP challenge and response packets it sends to the peer. This name defaults to the local hostname, or you can explicitly set it using the `local-name` option. When a host receives a CHAP challenge or CHAP response packet on a particular interface, it uses the peer identity to look up the CHAP secret key to use. For more information about `local-name` option, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

To configure CHAP, include the profile statement and specify a profile name at the [edit access] hierarchy level:

```
[edit access]
profile profile-name {
  client name chap-secret data;
}
```

Then reference the CHAP profile name at the [edit interfaces] hierarchy level. For more information about how to reference CHAP, see the *JUNOS Internet Software Configuration Guide: Interfaces and Class of Service*.

You can configure multiple profiles. You can also configure multiple clients for each profile.

profile is the mapping between peer identifiers and CHAP secret keys. The identity of the peer contained in the CHAP challenge or response queries the profile for the secret key to use.

client is the peer identity.

chap-secret secret is the secret associated with that peer.

Example: PPP Challenge Handshake Authentication Protocol

Configure the profile pe-A-ppp-clients at the [edit access] hierarchy level, then reference it at the [edit interfaces] hierarchy level.

```
[edit]
access {
  profile pe-A-ppp-clients {
    client cpe-1 chap-secret "$1$dQYsZ$B5ojUeUjDsUo.yKwcCZO"; # SECRET-DATA
    client cpe-2 chap-secret "$1$kdAsfaDAfkjDsASxfafdKdFKJ"; # SECRET-DATA
  }
}

interfaces {
  so-1/1/1 {
    encapsulation ppp;
    ppp-options {
      chap {
        access-profile pe-A-ppp-clients;
        local-name "pe-A-so-1/1/1";
      }
    }
  }
  so-1/1/2 {
    encapsulation ppp;
    ppp-options {
      chap {
        passive;
        access-profile pe-A-ppp-clients;
        local-name "pe-A-so-1/1/2";
      }
    }
  }
}
```

Configure the Authentication Order

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 the authentication order, include the authentication-order statement at the [edit access profile *profile-name*] hierarchy level:

```
[edit access profile profile-name]  
authentication-order [ authentication-methods ];
```

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

radius—Verify the client using RADIUS authentication services.

password—Verify the client using the information configured at the [edit access profile *profile-name* client *client-name*] hierarchy level.

If you do not include the authentication-order statement, clients are verified by means of password authentication.

The CHAP authentication sequence cannot take more than 30 seconds. If it takes longer than that to authenticate a client, the authentication is abandoned and a new sequence is initiated.

For example, if you configure three RADIUS servers such that the number of times the router attempts to contact each server is three times, and that with each retry the server times out after 3 seconds, then the maximum time given to the RADIUS authentication method before CHAP considers it a failure is 27 seconds. If you add more RADIUS servers to this configuration, they might not be contacted because the authentication process might be abandoned before these servers are tried.

The JUNOS software enforces a limit to the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—may fail to authenticate a client when this limit is exceeded. In the above example, any authentication method following this method is tried. If it fails, the authentication sequence is reinitiated by the router until authentication succeeds and the link is brought up.

RADIUS authentication servers are configured at the [edit system radius-server] hierarchy level. For more information about configuring RADIUS authentication servers, see “Configure RADIUS Authentication” on page 279.

Trace Access Processes

To trace access processes, you can specify options in the traceoptions statement at the [edit access] hierarchy level:

```
[edit access]
traceoptions {
  flag all;
  flag authentication;
  flag chap;
  flag configuration;
  flag radius;
}
```

You can specify the following access tracing flags:

- all—All tracing operations
- authentication—All authentication module-handling
- chap—All CHAP messages and handling
- configuration—Reading of configuration
- radius—All RADIUS messages and handling

Summary of Access Configuration Statements

The following sections explain each of the access configuration statements. The statements are organized alphabetically.

authentication-order

Syntax	authentication-order [<i>authentication-methods</i>];
Hierarchy Level	[edit access profile <i>profile-name</i>]
Description	Sets the order in which the JUNOS software tries different authentication methods when verifying that a client can access the router. For each login attempt, the software tries the authentication methods in order, from first to last.
Options	radius—Verify the client using RADIUS authentication services . password—Verify the client using the information configured at the [edit access profile <i>profile-name</i> client <i>client-name</i>] hierarchy level.
Usage Guidelines	See “Configure the Authentication Order” on page 403.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

client

Syntax	client <i>name</i> chap-secret <i>data</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i>]
Description	Name of the entity requesting access.
Options	<i>name</i> —Peer identity. chap-secret <i>data</i> —CHAP secret associated with the given peer identity.
Usage Guidelines	See “Configure the Authentication Order” on page 403.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration

profile

Syntax	profile <i>profile-name</i> { client <i>name</i> chap-secret <i>data</i> ; }
Hierarchy Level	[edit access]
Description	Configure PPP CHAP.
Options	profile <i>name</i> —Mapping between peer identifiers and CHAP secret keys. This is the entity that is queried for the secret key whenever a CHAP challenge or response is received.
Usage Guidelines	See “Configure Challenge Handshake Authentication Protocol” on page 401.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

traceoptions

Syntax	traceoptions { flag all; flag authentication; flag chap; flag configuration; flag radius; }
Hierarchy Level	[edit access]
Description	Configure access tracing options. To specify more than one tracing operation, include multiple flag statements.
Options	flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. all—All tracing operations

authentication—All authentication module-handling

chap—All CHAP messages and handling

configuration—Reading of configuration

radius—All RADIUS messages and handling

Usage Guidelines See “Trace Access Processes” on page 404.

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