Configuring the PPP Challenge Handshake Authentication Protocol

For interfaces with PPP encapsulation, you can configure interfaces to support the PPP Challenge Handshake Authentication Protocol (CHAP), as defined in RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*. When you enable CHAP on an interface, the interface can authenticate its peer and can be authenticated by its peer.

By default, PPP CHAP is disabled. If CHAP is not explicitly enabled, the interface makes no CHAP challenges and denies all incoming CHAP challenges. To enable CHAP, you must create an access profile, and you must configure the interfaces to use CHAP.

To configure a CHAP access profile, 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;
}
```

For more information about configuring access profiles, see the *JUNOS System Basics Configuration Guide*.

When you configure an interface to use CHAP, you must assign an access profile to the interface. When an interface receives CHAP challenges and responses, the access profile in the packet is used to look up the shared secret, as defined in RFC 1994.

If no matching access profile is found for the CHAP challenge that was received by the interface, the optionally configured default CHAP secret is used. The default CHAP secret is useful if the CHAP name of the peer is unknown, or if the CHAP name changes during PPP link negotiation.

To configure PPP CHAP on an interface with PPP encapsulation, include the **chap** statement at the [**edit interfaces** *interface-name* **ppp-options**] hierarchy level:

```
[edit interfaces interface-name ppp-options]
chap {
    access-profile name;
    default-chap-secret name;
    local-name name;
    [Unresolved xref];
}
```

On each interface with PPP encapsulation, you can configure the following PPP CHAP properties:

- Assigning an Access Profile to an Interface on page 2
- Configuring a Default CHAP Secret on page 2
- Configuring the Local Name on page 2

- Configuring Passive Mode on page 3
- Example: Configuring the PPP Challenge Handshake Authentication Protocol on page 3

When you configure PPP over ATM or Multilink PPP over ATM encapsulation, you can enable CHAP on the logical interface. For more information, see Configuring PPP over ATM2 Encapsulation.

Assigning an Access Profile to an Interface

To assign an access profile to an interface, include the access-profile statement at the [edit interfaces *interface-name* ppp-options chap] hierarchy level:

```
[edit interfaces interface-name ppp-options chap]
access-profile name;
```

You must include the access-profile statement when you configure the CHAP authentication method. If an interface receives a CHAP challenge or response from a peer that is not in the applied access profile, the link is immediately dropped unless a default CHAP secret has been configured. For information about configuring the default CHAP secret, see "Configuring a Default CHAP Secret" on page 2.

Configuring a Default CHAP Secret

To configure a default CHAP secret for an interface, include the default-chap-secret statement at the [edit interfaces *interface-name* ppp-options chap] hierarchy level:

```
[edit interfaces interface-name ppp-options chap]
default-chap-secret name;
```

The default CHAP secret is used when no matching CHAP access profile exists, or if the CHAP name changes during PPP link negotiation.

Configuring the Local Name

By default, when CHAP is enabled on an interface, the interface uses the routing platform's system hostname as the name sent in CHAP challenge and response packets.

To configure the name the interface uses in CHAP challenge and response packets, include the local-name statement at the [edit interfaces *interface-name* ppp-options chap] hierarchy level:

```
[edit interfaces interface-name ppp-options chap]
local-name name;
```

The local name is any string from 1 to 250 characters in length, starting with an alphanumeric or underscore character, and including only the following characters:

```
a-z A-Z 0-9 % @ # / \ . _ -
```

Configuring Passive Mode

By default, when CHAP is enabled on an interface, the interface always challenges its peer and responds to challenges from its peer.

You can configure the interface not to challenge its peer, and only respond when challenged. To configure the interface not to challenge its peer, include the **passive** statement at the [**edit interfaces** *interface-name* **ppp-options chap**] hierarchy level:

```
[edit interfaces interface-name ppp-options chap]
[Unresolved xref];
```

Example: Configuring the PPP Challenge Handshake Authentication Protocol

Configure CHAP:

```
[edit access]
profile pe-A-ppp-clients;
client cpe-1 chap-secret "$1$dQYsZ$B5ojUeUjDsUo.yKwcCZ0";
            # SECRET-DATA
client cpe-2 chap-secret "$1$kdAsfaDAfkdjDsASxfafdKdFKJ";
            # SECRET-DATA
[edit interfaces so-1/2/0]
encapsulation ppp;
ppp-options {
   chap {
      access-profile pe-A-ppp-clients;
      default-chap-secret "$9$mPafafhdsaiufhyrv1Rxd";
      local-name "pe-A-so-1/1/1";
   }
}
[edit interfaces so-1/1/2]
encapsulation ppp;
ppp-options {
   chap {
      access-profile pe-A-ppp-clients;
      default-chap-secret "$9$mPafafhdsaiufhyrv1Rxd";
      local-name “pe-A-so-1/1/2";
   }
}
```