Configuring the PPP Password Authentication Protocol

For interfaces with PPP encapsulation, you can configure interfaces to support the Password Authentication Protocol (PAP), as defined in RFC 1334, *PAP Authentication Protocols*. If authentication is configured, the PPP link negotiates using CHAP or PAP protocol for authentication during the Link Control Protocol (LCP) negotiation phase. PAP is only performed after the link establishment phase (LCP up) portion of the authentication phase.

During authentication, the PPP link sends a PAP authentication-request packet to the peer with an ID and password. The authentication-request packet is sent every 2 seconds, similar to the CHAP challenge, until a response is received (acknowledgment packet, nonacknowledgment packet). If an acknowledgment packet is received, the PPP link transitions to the next state, the network phase. If a nonacknowledgment packet is received, an LCP terminate request is sent, and the PPP link goes back to the link establishment phase. If no response is received, and an optional retry counter is set to true, a new request acknowledgment packet is resent. If the retry counter expires, the PPP link transitions to the LCP negotiate phrase.

You can configure the PPP link with PAP in passive mode. By default, when PAP is enabled on an interface, the interface always sends authenticate-request packets to the peer, and requires that the peer acknowledge the authenticate-request packets. In passive mode, the router with the PPP link configured for PAP authenticates any incoming connections, but will not require the peer to authenticate its connection.

Both CHAP and PAP authentication can be configured on a PPP interface. If both are configured, CHAP is negotiated first. If CHAP authentication fails, PAP authentication is negotiated.

To enable PAP, you must create an access profile, and you must configure the interfaces to use PAP.

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

```
[edit access]
profile profile-name {
    client name;
    pap-password password;
}
```

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

When you configure an interface to use PAP, you must assign an access profile to the interface. When an interface receives PAP authentication requests, the access profile in the packet is used to look up the password.

If no matching access profile is found for the PAP authentication request that was received by the interface, the optionally configured default PAP password is used.

For information about configuring the default PAP password, see Configuring PPP PAP Authentication.

To configure PPP PAP on a physical interface with PPP encapsulation, include the pap statement at the [edit interfaces *interface-name* ppp-options] hierarchy level:

```
[edit interfaces interface-name ppp-options]
pap {
    access-profile name;
    local-name name;
    local-password password;
    [Unresolved xref];
}
```

To configure PPP PAP on a logical interface with PPP encapsulation, include the pap statement with options:

```
pap {
    default-pap-password password;
    local-name name;
    local-password password;
    [Unresolved xref];
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

For more information about configuring PAP for logical interfaces, see Configuring PPP PAP Authentication. For information about configuring tracing operations for PPP, see Tracing Operations of the pppd Process.

On each physical interface with PPP encapsulation, you can perform one of the following tasks:

Configuring the Local Name

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

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

```
[edit interfaces interface-name ppp-options pap]
```

local-name *name*;

Configuring the Local Password

You need to configure the password to be used for authentication. To configure the host password for sending PAP requests, include the local-password statement at the [edit interfaces *interface-name* ppp-options pap] hierarchy level:

local-password *password*;

Configuring Passive Mode

By default, when PAP is enabled on an interface, the interface always sends authenticate-request packets to the peer, and requires that the peer acknowledge the authenticate-request packets. However, some peer routers may not support bidirectional authentication. In these cases, you can instead configure PAP to operate in passive mode. In passive mode, the router with the PPP link configured for PAP authenticates any incoming connections, but will not require the peer to authenticate its connection.

To configure the interface to authenticate with PAP in passive mode, include the passive statement at the [edit interfaces *interface-name* ppp-options pap] hierarchy level:

[edit interfaces *interface-name* ppp-options pap]
[Unresolved xref];

Example: Configuring PAP Authentication Protocol

Configure a PAP access profile, the physical and logical interfaces, and tracing operations for PPP.

For PAP authentication, a username and password for the peer is configured in the access profile, along with a PAP password. Each user can have either a PAP password or a CHAP secret.

```
[edit access]
profile userlist1;
client {
   papuser {
      pap-password "#%@^***"; # SECRET-DATA;
   }
   chapuser {
      chap-secret "#%@^***"; # SECRET-DATA;
   }
}
```

To configure the same name for the PAP password and the CHAP secret, configure the client with two different access profiles:

```
[edit access]
profile chap-profile;
client {
```

```
    sjcrouter {
        chap-secret "#%@^***"; # SECRET-DATA;
    }
    boston {
        chap-secret "#%@^***"; # SECRET-DATA;
    }
}
profile pap-profile;
client {
    sjcrouter {
        pap-password "#%@^***"; # SECRET-DATA;
    }
    boston {
        pap-password "#%@^***"; # SECRET-DATA;
    }
}
```

Configure the physical interface, including the access profile name to be used for PPP authentication:

```
[edit interfaces so-0/0/0]
ppp-options {
    pap {
        access-profile “pap-profile”;
        local-name "rtrnum1";
        local-password "XXXXXXX"; #SECRET-DATA
        passive;
    }
}
```

Configure the logical interface, including the default PAP password to be used, should the access profile not be located during authentication:

```
[edit interfaces so-0/0/0]
encapsulation frame-relay;
unit 0 {
    dlci 100;
    encapsulation frame-relay-ppp;
    ppp-options {
        pap {
            local-name "rtrnum1";
            local-password "XXXXXXX"; #SECRET-DATA
            default-pap-password "XXXXX"; #SECRET-DATA
            passive;
        }
    }
}
```

Include the **pap** statement to trace PPP protocol operations:

```
[edit protocols]
ppp {
    traceoptions {
        flag {
            pap;
        }
```

```
    }
}
```