PPP CHAP/PAP Authentication over an IPv6 Serial Link Configuration Example

Document ID: 113073

Contents

Introduction

This document provides a sample configuration for Point−to−Point Protocol (PPP) Challenge Handshake Authentication Protocol (CHAP)/ Password Authentication Protocol (PAP) Authentication over an IPv6 Serial Link.

When either PAP or CHAP is enabled, the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database. It uses the stored secret to encrypt the original challenge and verify that the encrypted values match.

Prerequisites

Requirements

Make sure that you meet these requirements before you attempt this configuration:

- Understand the PAP/CHAP authentication process
- Understand basic IPv6

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 12.4, Advance IP Services Feature Set
- Cisco 3700 Series Multiservice Access Routers

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

In the example, routers R1 and R2 are configured with PPP authentication. In router R1, the interface S1/0 is IPv6 enabled and has the IPv6 address **2011:2706:ABC::/64 eui−64** by implementing EUI−64. Extended Unique Identifier (EUI) enables the host to automatically assign itself a unique 64−bit IPv6 interface identifier without the need for manual configuration or DHCP. This is accomplished on Ethernet interfaces by referencing the already unique 48−bit MAC address, and reformatting that value to match the EUI−64 specification. Similarly, the S1/0 interface on router R2 is enabled with **2011:2706:ABC::/64 eui−64**.

Configure

Routers R1 and R2 are configured with basic PPP/CHAP authentication.

Network Diagram
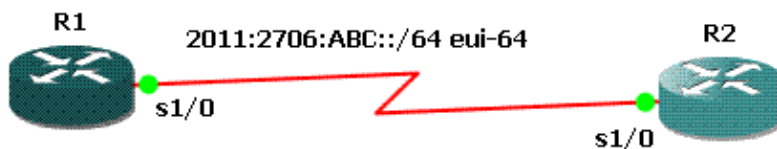
Configurations

This document uses these configurations:

- R1 Configuration
- R2 Configuration

R1 Configuration

```
hostname R1
!
aaa new-model
!
aaa authentication ppp default local
!
username R2 password 0 cisco

interface Serial1/0
 no ip address
 encapsulation ppp
 ipv6 address 2011:2706:ABC::/64 eui-64
```

```
ipv6 enable
no fair-queue
ppp authentication chap callin
!
```

R2 Configuration

```
interface Serial1/1
 no ip address
 encapsulation ppp
 ipv6 address 2011:2706:ABC::/64 eui-64
 ipv6 enable
 clock rate 64000
 ppp chap hostname R2
 ppp chap password 0 cisco
```

Verify

This section provides information you can use to confirm that your configuration works properly.

On router R1, issue these commands:

1. **debug ppp negotiation**

   debug ppp negotiation

   ```
   *Jun 27 08:34:56:357: Se1/0 PPP: Outbound cdp packet dropped
   *Jun 27 08:34:56:845: %SYS-5-CONFIG_|: Configured from console by console
   *Jun 27 08:34:58:357: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
   *Jun 27 08:34:58:357: Se1/0 PPP: Using default call direction
   *Jun 27 08:34:58:357: Se1/0 PPP: Treating connection as a dedicated line
   *Jun 27 08:34:58:357: Se1/0 PPP: Session handle[470002F8] Session id[29]
   *Jun 27 08:34:58:357: Se1/0 PPP: Phase is ESTABLISHING, Active Open
   *Jun 27 08:34:58:357: Se1/0 LCP: O CONFREQ [Closed] id 72 len 15
   *Jun 27 08:34:58:357: Se1/0 LCP:  AuthProto CHAP (0x0305C22305)
   *Jun 27 08:34:58:357: Se1/0 LCP:  MagicNumber 0x35B44C0F (0x050635B44C0F)
   *Jun 27 08:34:58:361: Se1/0 LCP: I CONFREQ {REQsent] id 59 len 10
   *Jun 27 08:34:58:361: Se1/0 LCP:  MagicNumber 0x1FEDF9A2 (0x05061FEDF9A2)
   *Jun 27 08:34:58:361: Se1/0 LCP: O CONFACK {REQsent] id 59 len 10
   *Jun 27 08:34:58:361: Se1/0 LCP:  MagicNumber 0x1FEDF9A2 (0x05061FEDF9A2)
   *Jun 27 08:34:58:365: Se1/0 LCP: I CONFACK {ACKsent] id 72 len 15
   *Jun 27 08:34:58:365: Se1/0 LCP:  AuthProto CHAP (0x0305C22305)
   *Jun 27 08:34:58.365: Se1/0 LCP:   MagicNumber 0x35B44C0F (0x050635B44C0F)
   *Jun 27 08:34:58.365: Se1/0 LCP: State is Open
   *Jun 27 08:34:58.365: Se1/0 PPP: Phase is AUTHENTICATING, by this end
   *Jun 27 08:34:58.365: Se1/0 CHAP: O CHALLENGE id 5 len 23 from "R1"
   *Jun 27 08:34:58.377: Se1/0 CHAP: I RESPONSE id 5 len 23 from "R2"
   *Jun 27 08:34:58.377: Se1/0 PPP: Phase is FORWARDING, Attempting Forward
   *Jun 27 08:34:58.377: Se1/0 PPP: Phase is AUTHENTICATING, Unauthenticated User
   *Jun 27 08:34:58.381: Se1/0 PPP: Phase is FORWARDING, Attempting Forward
   *Jun 27 08:34:58.381: Se1/0 PPP: Phase is AUTHENTICATING, Authenticated User
   *Jun 27 08:34:58.381: Se1/0 CHAP: O SUCCESS id 5 len 4
   *Jun 27 08:34:58.381: Se1/0 PPP: Phase is UP
   *Jun 27 08:34:58.381: Se1/0 CDPCP: O CONFREQ [Closed] id 1 len 4
   *Jun 27 08:34:58.381: Se1/0 IPV6CP: O CONFREQ [Closed] id 1 len 14
   *Jun 27 08:34:58.381: Se1/0 IPV6CP:    Interface-Id 021B:54FF:FEA9:24B0
       (0x010A021B54FFFEA924B0)
   *Jun 27 08:34:58.381: Se1/0 PPP: Process pending ncp packets
   *Jun 27 08:34:58.389: Se1/0 CDPCP: I CONFREQ [REQsent] id 1 len 4
   *Jun 27 08:34:58.389: Se1/0 CDPCP: O CONFACK [REQsent] id 1 len 4
   *Jun 27 08:34:58.389: Se1/0 IPV6CP: I CONFREQ [REQsent] id 1 len 14
   *Jun 27 08:34:58.389: Se1/0 IPV6CP:    Interface-Id 021F:CAFF:FE04:F918
   ```

```
        (0x010A021FCAFFFE04F918)
*Jun 27 08:34:58.389: Se1/0 IPV6CP: O CONFACK [REQsent] id 1 len 14
*Jun 27 08:34:58.389: Se1/0 IPV6CP:    Interface-Id 021F:CAFF:FE04:F918
        (0x010A021FCAFFFE04F918)
*Jun 27 08:34:58.393: Se1/0 CDPCP: I CONFACK [ACKsent] id 1 len 4
*Jun 27 08:34:58.393: Se1/0 CDPCP: State is Open
*Jun 27 08:34:58.393: Se1/0 IPV6CP: I CONFACK [ACKsent] id 1 len 14
*Jun 27 08:34:58.393: Se1/0 IPV6CP:    Interface-Id 021B:54FF:FEA9:24B0
        (0x010A021B54FFFEA924B0)
*Jun 27 08:34:58.393: Se1/0 IPV6CP: State is Open
*Jun 27 08:34:59.381: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0,
        changed state to up
```

2. **debug ppp authentication**

```
*Jun 27 08:37:46.045: Se1/0 PPP: Using default call direction
*Jun 27 08:37:46.045: Se1/0 PPP: Treating connection as a dedicated line
*Jun 27 08:37:46.045: Se1/0 PPP: Session handle[C40002F9] Session id[30]
*Jun 27 08:37:46.045: Se1/0 PPP: Authorization NOT required
*Jun 27 08:37:46.053: Se1/0 CHAP: O CHALLENGE id 6 len 23 from "R1"
*Jun 27 08:37:46.065: Se1/0 CHAP: I RESPONSE id 6 len 23 from "R2"
*Jun 27 08:37:46.065: Se1/0 PPP: Sent CHAP LOGIN Request
*Jun 27 08:37:46.065: Se1/0 PPP: Received LOGIN Response PASS
*Jun 27 08:37:46.069: Se1/0 CHAP: O SUCCESS id 6 len 4
```

On router R2, issue this command:

- **debug ppp authentication**

  debug ppp authentication

```
*Feb 28 05:18:39.439: Se1/1 PPP: Using default call direction
*Feb 28 05:18:39.439: Se1/1 PPP: Treating connection as a dedicated line
*Feb 28 05:18:39.439: Se1/1 PPP: Session handle[E300000B] Session id[35]
*Feb 28 05:18:39.439: Se1/1 PPP: Authorization required
*Feb 28 05:18:39.451: Se1/1 PPP: No authorization without authentication
*Feb 28 05:18:39.455: Se1/1 CHAP: I CHALLENGE id 7 len 23 from "R1"
*Feb 28 05:18:39.459: Se1/1 CHAP: Using hostname from interface CHAP
*Feb 28 05:18:39.459: Se1/1 CHAP: Using password from interface CHAP
*Feb 28 05:18:39.459: Se1/1 CHAP: O RESPONSE id 7 len 23 from "R2"
*Feb 28 05:18:39.467: Se1/1 CHAP: I SUCCESS id 7 len 4
```

Related Information

- **IP Version 6 Support Page**
- **Implementing IPv6 Addressing and Basic Connectivity**
- **IP Routing Support Page**
- **Technical Support & Documentation – Cisco Systems**