

# Connect a CPA 75X Bridge and CPA 75X IPX Router using PPP PAP

Document ID: 47885

---

## Introduction

### Prerequisites

- Requirements

- Components Used

- Conventions

### Configure

- Network Diagram

- Configurations

### Verify

### Troubleshoot

### Related Information

---

## Introduction

This document provides a sample configuration for connecting a CPA 75x bridge to a CPA 75x IP router using Point-to-Point Protocol (PPP) Password Authentication Protocol (PAP) on IPX networks.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on the CPA 75x bridge and IP router.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

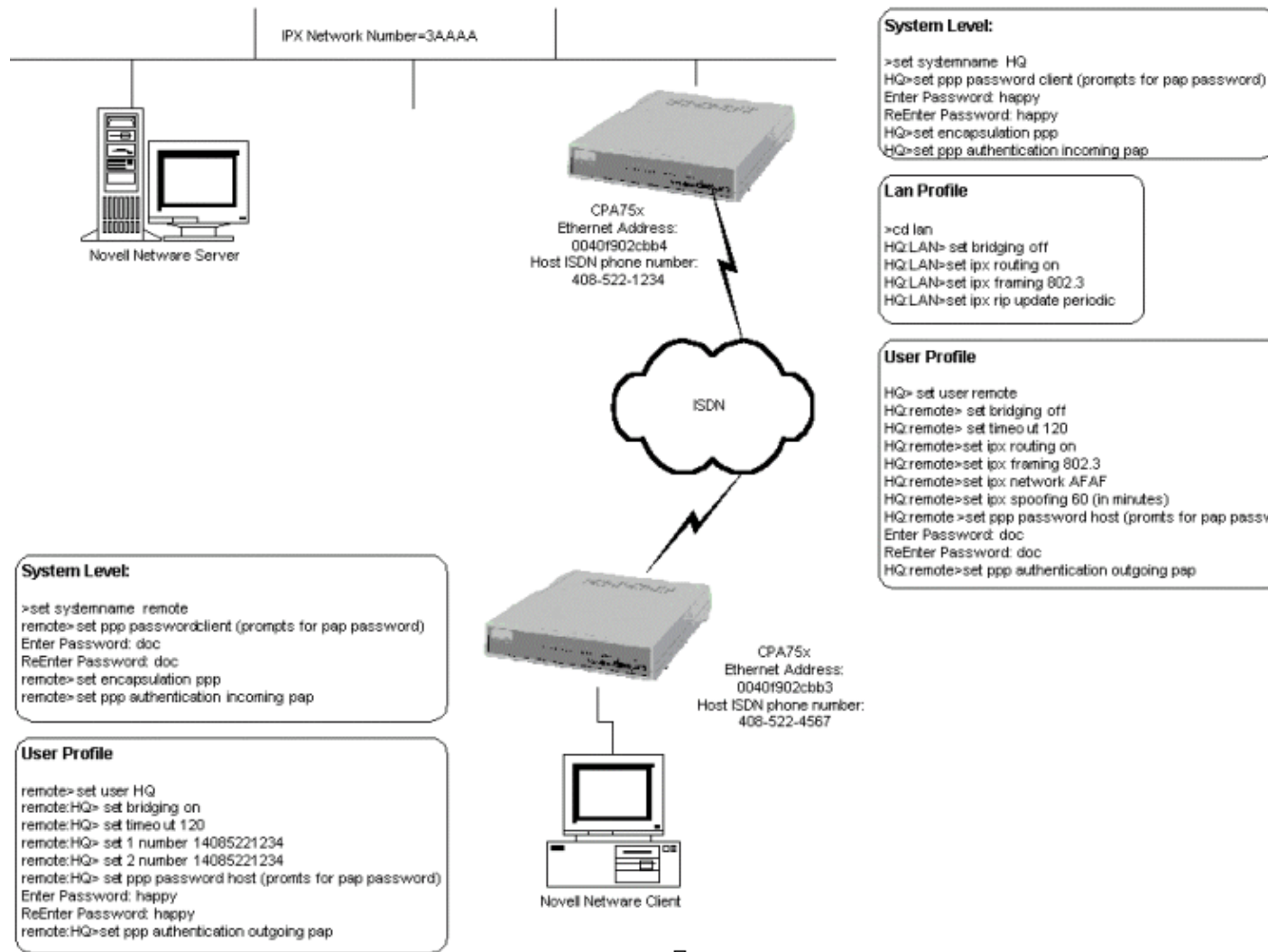
## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** To find additional information on the commands used in this document, use the Command Lookup Tool ( registered customers only) .

# Network Diagram

This document uses this network setup:



## Configurations

This document uses these configurations:

- Main Site Router
- Remote Router

Main Site Router
<pre>&gt;set systemname HQ  !--- Sets the system name of the main router. !--- This system name "HQ" must match the user profile in the remote !--- site router for authentication purposes. The system name is sent to !--- the far end router as the userid during PPP authentication.  HQ&gt;set ppp secret client (prompts for PAP password)  !--- Sets the PAP password !--- sent to the remote router when the remote router challenges !--- the main router.</pre>

```
Enter Password: happy

!--- Prompted to enter the password/secret.
!--- Enter "happy" as the PAP password.

ReEnter Password: happy

!--- Prompted to re-enter the password/secret to ensure consistency.

HQ>set encapsulation ppp

!--- Sets the encapsulation for the user profile default template to PPP.

HQ>set ppp authentication incoming pap

!--- Sets the PPP authentication for incoming calls to use PAP.

HQ>cd lan

!--- Change to LAN profile.

HQ:LAN>set bridging off

!--- Turns bridging off in the LAN profile.

HQ:LAN>set ipx routing on

!--- Turns IPX routing on.

HQ:LAN>set ipx framing 802.3

!--- Sets the IPX framing type to 802.3.

HQ:LAN>set ipx rip update periodic

!--- Sends the ipx rip and sap tables out the ethernet port every 60 seconds.

HQ:LAN>set user remote

!--- Creates the user profile "remote". Changes to the user profile "remote".
!--- This user profile name must match the system name of the remote
!--- site router. The system name is received from the far end as the userid
!--- during PPP authentication.

HQ:remote>set bridging off

!--- Turns bridging off in the user profile "remote".

HQ:remote>set timeout 120

!--- Sets the idle timeout parameter to 120 seconds. If there is no
!--- interesting traffic to be forwarded across the ISDN connection for 120
!--- seconds then the call is disconnected. Because the ipx rip updates are
!--- periodic by default on the user profile, the call will never disconnect.
!--- There are no ipx filters available at this time.

HQ:remote>set ipx routing on

!--- Turns ipx routing on in the user profile "remote".

HQ:remote>set ipx framing 802.3

!--- Sets ipx framing type to 802.3.

HQ:remote>set ipx network AFAF
```

```

!--- Sets the ipx network number of the user profile "remote".
!--- Note: The far end router is in the same ipx network as this interface.

HQ:remote>set ipx spoofing 60 (in minutes)

!--- Sets the ipx watchdog spoofing to 60 minutes. If the call disconnects,
!--- the users' logins will be spoofed to the main site servers for 60 minutes.
!--- If the connection is not made before the 60 minutes, then the spoofing ends
!--- and the router will no longer answer the server's watchdog packets.
!--- At this point the user's session will be closed.

HQ:remote>set ppp password host (prompts for pap password)

!--- Sets the pap secret that the main router is expecting the remote router
!--- to send when the main router challenges the remote router to authenticate.

Enter Password: doc

!--- Prompted to enter password/secret.
!--- Enter "doc" as the PAP password.

ReEnter Password: doc

!--- Prompted to re-enter password/secret.

HQ:remote>set ppp authentication outgoing PAP

!--- Sets the PPP authentication on outbound calls to PAP.
!--- This setting will force bi-directional authentication using PAP on the
!--- outgoing call basis. When the main router calls the remote router,
!--- the main router will force the remote router to authenticate with
!--- it using PAP.

```

### Remote Router

```

>set systemname remote

!--- Sets the system name of the remote router.
!--- This system name "remote" must match the user profile in the main
!--- site router for authentication purposes. The system name is sent to the
!--- far end router as the userid in PPP authentication.

remote>set ppp password client (prompts for PAP password)

!--- Sets the PAP password used to send the PAP magic number
!--- to the main router when the main router challenges the remote router.

Enter Password: doc

!--- Prompted to enter the password/secret. Enter "doc" as the PAP password.

ReEnter Password: doc

!--- Prompted to re-enter password/secret.

remote>set encapsulation ppp

!--- Sets the encapsulation for the user profile default template to PPP.

remote>set ppp authentication incoming PAP

!--- Sets the PPP authentication for incoming calls to be forced to authenticate
!--- using PAP.

```

```
remote>set user HQ

!--- Creates the user profile "HQ". Changes to the user profile "HQ".
!--- This user profile name has to match the system name of the main site router.
!--- The system name is received from the far end as the userid during
!--- PPP authentication.

remote:HQ>set bridging on

!--- Turns bridging on in the user profile "HQ".

remote:HQ>set timeout 120

!--- Sets the idle timeout parameter to 120 seconds.
!--- If there is no interesting traffic to be forwarded across the ISDN
!--- connection for 120 seconds then the call is disconnected.
!--- Because the IPX RIP updates are periodic by default on the user profile,
!--- the call will never disconnect.
!--- There are no IPX filters available at this time.

remote:HQ>set 1 number 14085221234

!--- Sets the phone numbers in the user profile "HQ" that are used to dial
!--- out to the main router. In this case, the main router has the same phone
!--- number for both b channels, so the same number is set in link 1 and link 2.
!--- Link 2 is for bandwidth on demand. It will not automatically connect if
!--- link 1 isn't already connected.
!--- Link 2's number is NOT used for a secondary dial number, it is for
!--- bandwidth on demand only.

remote:HQ>set 2 number 14085221234

!--- Note: In this scenario, the main router is not dialing out to
!--- the remote router. If it is necessary for the main router to call out
!--- to the remote router, then add "set 1 number" and "set 2 number" to
!--- the user profile "remote" with the phone numbers for the remote router.

remote:HQ>set ppp password host (prompts for pap password)

!--- Sets the pap password that will sent to the remote router when
!--- the remote router challenges the main router.

Enter Password: happy

!--- Prompted to enter the password/secret.
!--- Enter "happy" as the PAP password.

ReEnter Password: happy

!--- Prompted to re-enter the password/secret to ensure consistency.

remote:HQ>set ppp authentication outgoing PAP

!--- Sets the PPP authentication on outbound calls to PAP.
!--- This setting forces bi-directional authentication using PAP on the outgoing
!--- call basis. When the remote router calls the main router, the remote router
!--- forces the main router to authenticate with it using PAP.
```

## Verify

There is currently no verification procedure available for this configuration.

# Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

---

## Related Information

- [Access Product Support Pages](#)
  - [Technical Support – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 25, 2008

Document ID: 47885

---