

ISDN Configuration Example – IPX

Document ID: 10345

Introduction

Prerequisites

- Requirements

- Conventions

Configure

- Sample Configuration for C2503

- Network Diagram

- Explanation of C2503 Configuration

- Sample Configuration for C4000

- Explanation of C4000 Configuration

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This document provides a sample configuration and explanation of configuration for C2503 and C4000.

Prerequisites

Requirements

There are no specific requirements for this document.

Conventions

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

Configure

This section provides a sample configuration and explanation of configuration for C2503 and C4000.

Sample Configuration for C2503

In this section, you are presented with the information to configure the features described in this document for C2503.

```
C2503#wr t
#####
Current configuration:
!
version 10.2
!
hostname C2503
!
enable password test
!
```

```

username C4000 password cisco (See username explanation in the following
                               section.)

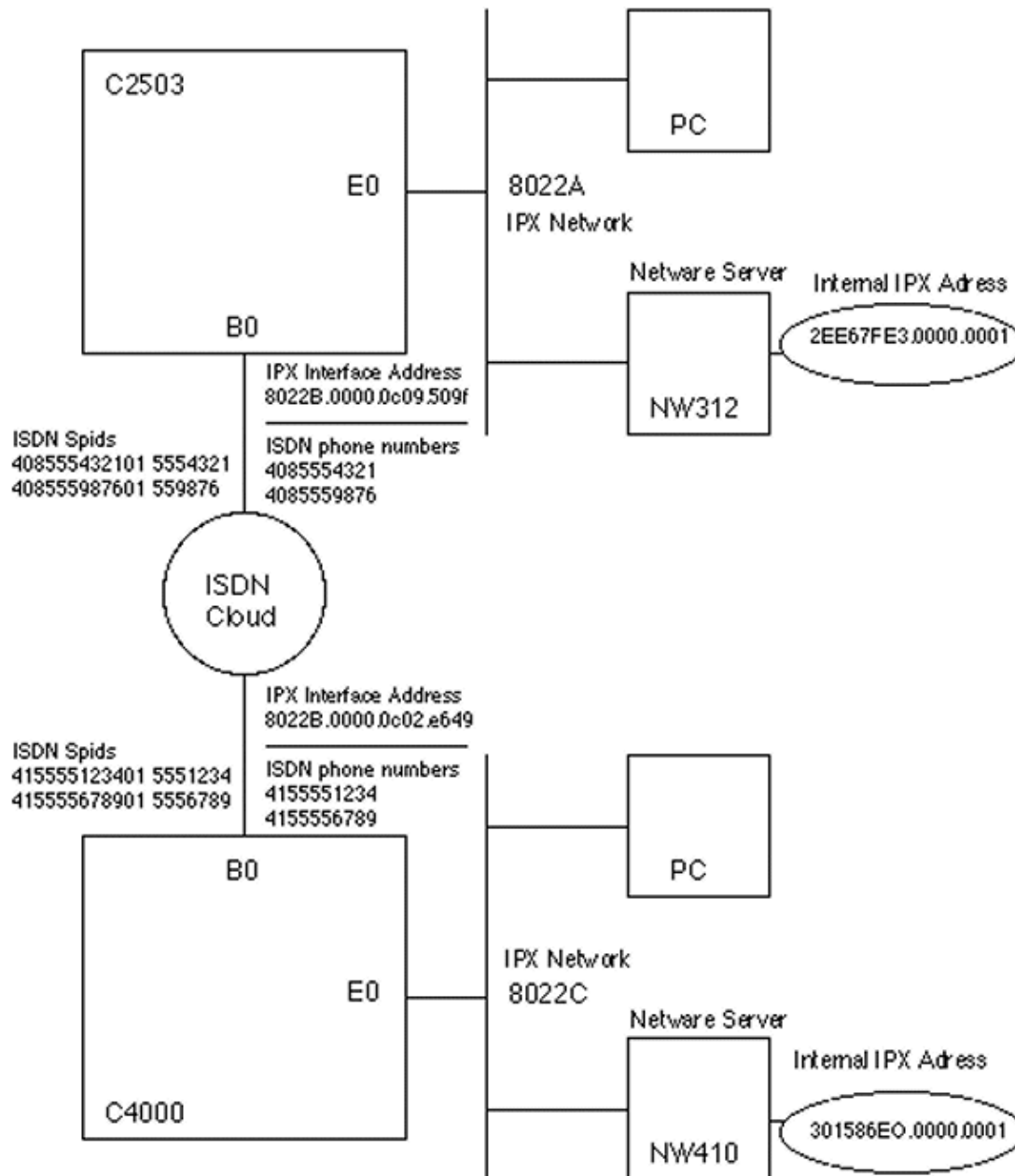
ipx routing 0000.0c09.509f
ipx gns-response-delay 1000
isdn switch-type basic-dms100
!
interface Ethernet0
ipx network 8022A
ipx encapsulation SAP
!
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
encapsulation ppp
bandwidth 56
ipx network 8022B
no ipx route-cache
ipx watchdog-spoof
dialer idle-timeout 300
dialer map ipx 8022B.0000.0c02.e649 name C4000 speed 56 broadcast
1415551234
dialer map ipx 8022B.0000.0c02.e649 name C4000 speed 56 broadcast
1415556789
dialer hold-queue 5
dialer load-threshold 100
dialer-group 1
isdn spid1 408555432101 5554321
isdn spid2 408555987601 5559876
ppp authentication chap
!
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 453
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 900 permit -1
ipx route 8022C 8022B.0000.0c02.e649
ipx route 301586E0 8022B.0000.0c02.e649
!
ipx sap 4 NW410 301586E0.0000.0000.0001 451 2
!
!
dialer-list 1 list 900
!
line con 0
line aux 0
line vty 0 4
password test
login
!
end

```

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Explanation of C2503 Configuration

```
C2503#wr t
#####
Current configuration:
!
version 10.2
!
hostname C2503
!
enable password test
!
username C4000 password cisco
```

The username "C4000" is the hostname of the remote router and is used by the **dialer map** command. The username is case sensitive and must match the hostname of the remote router exactly.

The password, which is used by the CHAP authentication process, is case sensitive and must match the remote router's password exactly.

Note: In order to avoid confusion, the *unencrypted* form of the password **cisco** is shown in this sample configuration. In the actual configuration, the password would appear in its encrypted form: **7 13061E010803**, where **7** denotes the encryption type, and **13061E010803** is the encrypted form of the password **cisco**. When you enter or make changes to the **username** command, always type the password in its *unencrypted* form, and do not enter the encryption type (**7**). It is set automatically.

```
ipx routing 0000.0c09.509f
```

This command enables IPX routing. The router chooses a MAC address from one of its interfaces to associate with the process, so you do not need to specify it with the command. Simply enter the command **ipx routing**.

```
ipx gns-response-delay 1000
```

The static SAP command advertises the remote server even when the ISDN link is not active. It can be necessary to increase the period of time before the router replies to the Get Nearest Server (GNS) request of a workstation in order to ensure that the local file server can respond first.

```
isdn switch-type basic-dms100
```

The ISDN switch type must match the equipment of your carrier. If you change the switch-type, you must reload the router for the new switch type to take effect.

```
interface Ethernet0
ipx network 8022A
```

8022A = the network number of the local network. In order to determine this number, type **config** at the console prompt of the local server and use the LAN protocol network number. You do not need to include the leading zeros displayed for the LAN protocol network number with this command.

```
ipx encapsulation SAP
```

This command sets the Ethernet frame type of the interface to match that of the local file server. In order to determine the frame type of the server, type **config** at the console prompt at the local server and use the Frame type specified.

Cisco supports these frame types:

Novell Frame Type	Cisco Encapsulation
Novell Ethernet_II	arpa
Novell Ethernet_802.3	novell-ether
IEEE 802.2	sap
IEEE 802.2 SNAP	snap

If you run a 3.11 (or earlier) file server, your frame type can be Ethernet 802.3. The router defaults to 802.3. In order to verify what frame type you have, check the autoexc.ncf file of the file server.

```
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
encapsulation ppp
```

PPP encapsulation is recommended over HDLC in order to allow the use of CHAP authentication.

```
bandwidth 56
```

The default bandwidth setting for a BRI interface is 64k. If you configure your dialer map statements with the speed 56 option, you must include the bandwidth statement.

Note: This command does not control the speed of your ISDN line. It sets the correct reference point for the show interface statistics of the BRI port, for the **dialer load-threshold** command, and for the IGRP/EIGRP routing metrics.

```
ipx network 8022B
```

8022B = the IPX network number of the ISDN segment for both routers. This network number must be unique to your internetwork.

```
no ipx route-cache
```

The IPX route cache must be turned off when the IPX watchdog spoofing is enabled.

```
ipx watchdog-spoof
```

This command enables the router to reply to the watchdog packets of the local server on behalf of the remote client. Without it, the watchdog packets of the server would be seen as *interesting* packets and would activate the ISDN link.

```
dialer idle-timeout 300
```

This command sets the number of seconds the ISDN connection remains open if no *interesting* traffic is routed. The timer is reset each time an *interesting* packet is forwarded

```
dialer map ipx 8022B.0000.0c02.e649 name C4000 speed 56 broadcast 14155551234  
dialer map ipx 8022B.0000.0c02.e649 name C4000 speed 56 broadcast 14155556789
```

The **dialer map** command is used with CHAP authentication to place the initial call to the remote router when *interesting* traffic is forwarded to the BRI interface. Once the connection is active, the **dialer idle-timeout** command determines how long it remains active. A dialer map statement is required for each ISDN phone number that is called. Be aware, though, that two dialer map statements that point to the same location can activate both B channels when you only want to use one channel.

Note: The command parameters for this example:

8022B.0000.0c02.e649 = the IPX address of the BRI interface of the remote router. In order to determine this address, type **show ipx interface B 0** at the console prompt of the remote router.

name C4000 = the hostname of the remote router. The name is case sensitive and should match the name configured for the **username** command.

speed 56 = sets the dialer speed to 56k for ISDN circuits that are not 64k end-to-end, and it must be included in the dialer map statements of both routers. Most installations in North America must be configured for 56K.

broadcast = allows the broadcast packets to be forwarded. Unless broadcast packets are specified as *interesting* packets by the **dialer-list** command, they are only forwarded when the ISDN link is active.

14155551234

1415556789 = the ISDN telephone numbers of the remote router.

```
dialer hold-queue 5
```

This command allows *interesting* packets to be queued until the ISDN connection is established. It is especially useful when a NetWare log on is used to activate the connection to prevent the workstation from timing out. In this example, five *interesting* packets are queued.

```
dialer load-threshold 100
```

This command is used to configure bandwidth on demand when it sets the maximum load before the dialer places another call through the second B channel. The load is the calculated weighted average load value for the interface, where 1 is unloaded and 255 is fully loaded. The actual load value you configure depends on the characteristics of your particular network. In this example, the second B channel is activated when the load reaches 39% of maximum utilization, which is 100 divided by 255.

```
dialer-group 1
```

The **dialer-group 1** command enables the dialer-list 1 on the BRI interface, which determines which packets are *interesting* and activate the ISDN connection.

```
isdn spid1 408555432101 5554321
isdn spid2 408555987601 5559876
```

The **isdn spid** commands are used if your carrier assigns spids to your ISDN lines.

```
ppp authentication chap
```

This command enables CHAP authentication.

```
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 453
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 900 permit -1
```

This access list determines which IPX packets are *interesting* and activate the ISDN link. The access-list you create depends on your particular network design.

Note: The command parameters for this example:

access-list 900 deny -1 -1 0 -1 452	defines all SAP packets as uninteresting.
access-list 900 deny -1 -1 0 -1 453	defines all RIP packets as uninteresting.
access-list 900 deny -1 -1 0 -1 457	defines all security packets as uninteresting.
access-list 900 permit -1	defines all other packets as interesting.

```
ipx route 8022C 8022B.0000.0c02.e649
```

This command creates a static route to the Ethernet network of the remote router through the BRI interface of the remote router. This is necessary because dynamic routes are removed when the ISDN link is down.

Note: The command parameters for this example:

8022C = the external IPX network number of the remote network. In order to determine this number, type

config at the console prompt of the remote server and use the LAN protocol statement.

8022B.0000.0c02.e649 = the IPX address of the BRI interface of the remote router. In order to determine this address, type **show ipx interface B 0** at the console prompt of the remote router.

```
ipx route 301586E0 8022B.0000.0c02.e649
```

This **ipx route** command creates a static route to the remote server through the BRI interface of the remote router. This is required because dynamic routes are lost when the ISDN link is down.

Note: The command parameters for this example:

301586E0 = the network portion of the internal IPX address of the remote server. In order to determine this address, type **show ipx servers** at the console prompt of the remote router.

8022B.0000.0c02.e649 = the IPX address of the BRI interface of the remote router. In order to determine this address, type **show ipx interface B 0** at the console prompt of the remote router.

```
ipx sap 4 NW410 301586E0.0000.0000.0001 451 2
```

This command creates a static SAP entry for the remote server which the local router advertises even when the ISDN link is not active.

Note: The command parameters for this example:

4 = SAP type (server)

NW410 = name of SAP service

301586E0.0000.0000.0001 = internal IPX network and host address of remote server. In order to determine this address, type **show ipx servers** at the console prompt of the remote router.

451 = socket (port) number of remote server, which is determined by the command **show ipx servers** on the remote router

2 = RIP hop count to the remote server

```
dialer-list 1 list 900
```

This command points to access-list 900, which determines which IPX packets are *interesting*.

```
line con 0
line aux 0
line vty 0 4
password test
login
!
end
```

Sample Configuration for C4000

In this section, you are presented with the information to configure the features described in this document for C4000.

```
C4000#wr t
```

```
#####
Current configuration:
!
version 10.2
!
hostname C4000
!
enable password test
!
username C2503 password cisco (See username explanation in the following
                               section)

ipx routing 0000.0c02.e649
ipx gns-response-delay 1000
isdn switch-type basic-dms100
!
interface Ethernet0
ipx network 8022C
ipx encapsulation SAP
!
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
encapsulation ppp
bandwidth 56
ipx network 8022B
no ipx route-cache
ipx watchdog-spoof
dialer idle-timeout 300
dialer map ipx 8022B.0000.0c09.509f name C2503 speed 56 broadcast 14085554321
dialer map ipx 8022B.0000.0c09.509f name C2503 speed 56 broadcast 14085559876
dialer hold-queue 5
dialer load-threshold 100
dialer-group 1
isdn spid1 415555123401 5551234
isdn spid2 415555678901 5556789
ppp authentication chap
!
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 453
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 900 permit -1
ipx route 8022A 8022B.0000.0c09.509f
ipx route 2EE67FE3 8022B.0000.0c09.509f
!
ipx sap 4 NW312 2EE67FE3.0000.0000.0001 451 2
!
!
dialer-list 1 list 900
!
line con 0
line aux 0
line vty 0 4
password test
login
!
end
```

Explanation of C4000 Configuration

```
C4000#wr t
#####
Current configuration:
!
version 10.2
!
hostname C4000
!
enable password test
!
username C2503 password cisco
```

The username "C4000" is the hostname of the remote router and is used by the **dialer map** command. The username is case sensitive and must match the hostname of the remote router exactly.

The password, which is used by the CHAP authentication process, is case sensitive and must match the password of the remote router exactly.

Note: In order to avoid confusion, the *unencrypted* form of the password cisco is shown in this sample configuration. In the actual configuration, the password appears in its encrypted form: **7 13061E010803**, where **7** denotes the encryption type and **13061E010803** is the encrypted form of the password **cisco**. When you enter or make changes to the **username** command, always type the password in its *unencrypted* form and do not enter the encryption type (**7**). It is set automatically.

```
ipx routing 0000.0c02.e649
```

This command enables IPX routing. The router chooses a MAC address from one of its interfaces to associate with the process, so you do not need to specify it with the command. Simply enter the command **ipx routing**.

```
ipx gns-response-delay 1000
```

The static SAP command advertises the remote server even when the ISDN link is not active. It can be necessary to increase the period of time before the router replies to the Get Nearest Server (GNS) request of a workstation to ensure that the local file server can respond first.

```
isdn switch-type basic-dms100
```

The ISDN switch type must match the equipment of your carrier. If you change the switch-type, you must reload the router in order for the new switch type to take effect.

```
interface Ethernet0
ipx network 8022C
```

8022C = the network number of the local network. In order to determine this number, type **config** at the console prompt of the local server and use the *LAN protocol* network number. You do not need to include the leading zeros displayed for the *LAN protocol* network number with this command.

```
ipx encapsulation SAP
```

This command sets the Ethernet frame type of the interface to match that of the local file server. In order to determine the frame type of the server, type **config** at the console prompt of the local server and use the *Frame* type specified.

Cisco supports these frame types:

Novell Frame Type	Cisco Encapsulation
Novell Ethernet_II	arpa
Novell Ethernet_802.3	novell-ether
IEEE 802.2	sap
IEEE 802.2 SNAP	snap

If you run a 3.11 (or earlier) file server, your frame type can be Ethernet 802.3. The router defaults to 802.3. In order to verify what frame type you have, check the autoexc.ncf file of the file server.

```
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
encapsulation ppp
```

PPP encapsulation is recommended over HDLC in order to allow the use of CHAP authentication.

```
bandwidth 56
```

The default bandwidth setting for a BRI interface is 64k. If you configure your dialer map statements with the speed 56 option, you must include the bandwidth statement.

Note: This command does not control the speed of your ISDN line. It sets the correct reference point for the show interface statistics of the BRI port, for the **dialer load-threshold** command, and for IGRP/EIGRP routing metrics.

```
ipx network 8022B
```

8022B = the IPX network number of the ISDN segment for both routers. This network number must be unique to your internetwork.

```
no ipx route-cache
```

IPX route cache must be turned off when IPX watchdog spoofing is enabled.

```
ipx watchdog-spoof
```

This command enables the router to reply to the watchdog packets of the local server on behalf of the remote client. Without it, the watchdog packets of the server are seen as interesting packets and activate the ISDN link.

```
dialer idle-timeout 300
```

This command sets the number of seconds the ISDN connection remains open if no interesting traffic is routed. The timer is reset each time an interesting packet is forwarded.

```
dialer map ipx 8022B.0000.0c09.509f name C2503 speed 56 broadcast 14085554321
dialer map ipx 8022B.0000.0c09.509f name C2503 speed 56 broadcast 14085559876
```

The **dialer map** command is used with CHAP authentication to place the initial call to the remote router when interesting traffic is forwarded to the BRI interface. Once the connection is active, the **dialer idle-timeout** command determines how long it remains active. A dialer map statement is required for each ISDN phone number that is called. Be aware though, that two dialer map statements *that point to the same location* can activate both B channels when you only want to use one channel.

Note: The command parameters for this example:

8022B.0000.0c09.509f = the IPX address of the BRI interface of the remote router. In order to determine this address, type **show ipx interface B 0** at the console prompt of the remote router.

name C2503 = the hostname of the remote router. The name is case sensitive and should match the name configured for the "username" command.

speed 56 = sets the dialer speed to 56k for ISDN circuits that are not 64k end-to-end, and must be included in the dialer map statements of both routers. Most installations in North America must be configured for 56K.

broadcast = allows the broadcast packets to be forwarded. Unless broadcast packets are specified as interesting packets by the "dialer-list" command, they are only forwarded when the ISDN link is active.

14085554321

14085559876 = the ISDN telephone numbers of the remote router.

```
dialer hold-queue 5
```

This command allows *interesting* packets to be queued until the ISDN connection is established. It is especially useful when a NetWare log on is used to activate the connection to prevent the workstation from timing out. In this example, five interesting packets are queued.

```
dialer load-threshold 100
```

This command is used to configure bandwidth on demand when it sets the maximum load before the dialer places another call through the second B channel. The load is the calculated weighted average load value for the interface, where 1 is unloaded and 255 is fully loaded. The actual load value you configure depends on the characteristics of your particular network. In this example, the second B channel is activated when the load reaches 39% of maximum utilization, which is 100 divided by 255.

```
dialer-group 1
```

The **dialer-group 1** command enables the dialer-list 1 on the BRI interface.

```
isdn spid1 408555432101 5554321
isdn spid2 408555987601 5559876
```

The **isdn spid** commands are used if your carrier assigns spids to your ISDN lines.

```
ppp authentication chap
```

This command enables CHAP authentication.

```
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 453
```

```
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 900 permit -1
```

This access list determines which IPX packets are interesting and activates the ISDN link. The access-list you create depends on your particular network design.

Note: The command parameters for this example:

```
access-list 900 deny -1 -1 0 -1 452    defines all SAP packets as
                                         uninteresting.
access-list 900 deny -1 -1 0 -1 453    defines all RIP packets to be
                                         uninteresting.
access-list 900 deny -1 -1 0 -1 457    defines all security packets as
                                         uninteresting.
access-list 900 permit -1              defines all other packets as
                                         interesting.
```

```
ipx route 8022A 8022B.0000. 0c09.509f
```

This command creates a static route to the Ethernet network of the remote router through the BRI interface of the remote router. This is necessary because dynamic routes are removed when the ISDN link is down.

Note: The command parameters for this example:

8022A = the external IPX network number of the remote network. In order to determine this number, type **config** at the console prompt of the remote server and use the LAN protocol statement.

8022B.0000.0c09.509f = the IPX address of the BRI interface of the remote router. In order to determine this address, type **show ipx interface B 0** at the console prompt of the remote router.

```
ipx route 2EE67FE3 8022B.0000.0c09.509f
```

This **ipx route** command creates a static route to the remote server through the BRI interface of the remote router. This is required because dynamic routes are lost when the ISDN link is down.

Note: The command parameters for this example:

2EE67FE3 = the network portion of the internal IPX address of the remote server. In order to determine this address, type **show ipx servers** at the console prompt of the remote router.

8022B.0000.0c09.509f = the IPX address of the BRI interface of the remote router. In order to determine this address, type **show ipx interface B 0** at the console prompt of the remote router.

```
ipx sap 4 NW312 2EE67FE3.0000.0000.0001 451 2
```

This command creates a static SAP entry for the remote server which the local router advertises even when the ISDN link is not active.

Note: The command parameters for this example:

4 = SAP type (server)

NW312 = name of SAP service

2EE67FE3.0000.0000.0001 = internal IPX network and host address of remote server. In order to determine this address, type **show ipx servers** at the console prompt of the remote router.

451 = socket (port) number of remote server, which is determined by the command **show ipx servers** on the remote router

2 = RIP hop count to the remote server

```
dialer-list 1 list 900
```

This command points to access-list 900 which determines which IPX packets are interesting.

```
line con 0
line aux 0
line vty 0 4
password test
login
!
end
```

Verify

There is currently no verification procedure available for this configuration.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

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

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Related Information

- [Technical Support & Documentation – 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: Oct 04, 2005

Document ID: 10345
