

# Configuring IPX Over ISDN

Document ID: 10598

---

## Introduction

### Prerequisites

- Requirements

- Conventions

### Configure

- Network Diagram

- Configurations

- C2503 Configuration Explanation

- C4000 Configuration Explanation

### Troubleshooting ISDN Connectivity

- Debugging Physical Connectivity

- Debugging SPIDS

- Testing for CHAP Authentication

- Call Setup Debug Messages

### Related Information

---

## Introduction

This document describes how to configure IPX on Cisco routers that communicate over an ISDN connection. Additionally, this document provides a detailed explanation of the configurations, as well as troubleshooting tips.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Conventions

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

## Configure

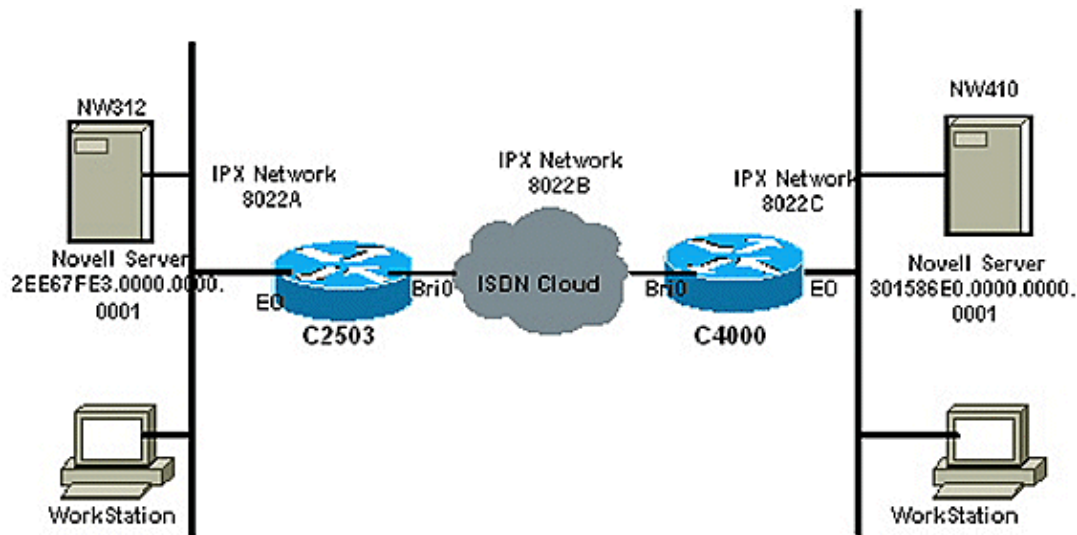
This section contains configurations for the Cisco 2503 and the Cisco 4000. Additionally, each configuration is explained in detail in the configuration explanation sections.

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

**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:



## Configurations

This document uses these configurations:

- C2503 Configuration
- C4000 Configuration
- C2503 Configuration Explanation
- C4000 Configuration Explanation

### C2503 Configuration

```

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

ipx routing 0000.0c09.509f
ipx gns-response-delay 1000
isdn switch-type basic-5ess

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
14155551234
dialer map ipx 8022B.0000.0c02.e649 name C4000 speed 56 broadcast
14155556789
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 protocol ipx list 900!
line con 0
line aux 0
line vty 0 4
password test
login
!
end

```

### C4000 Configuration

```

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

ipx routing 0000.0c02.e649
ipx gns-response-delay 1000
isdn switch-type basic-5ess
!
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 protocol ipx list 900!
line con 0
line aux 0
line vty 0 4
password test
login
!
end

```

## C2503 Configuration Explanation

The C2503 configuration is repeated in this section along with detailed explanations of many of the commands.

```

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 Challenge Handshake Authentication Protocol (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 0000.0c09.509f
```

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 a *Get Nearest Server* (GNS) request of a workstation to ensure that the local file server can respond first.

```
isdn switch-type basic-5ess
```

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 is 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.

The configuration continues:

```
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 Interior Gateway Routing Protocol/Enhanced Interior Gateway Routing Protocol (IGRP/EIGRP) routing metrics.

```
ipx network 8022B
```

8022B is 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.0000.0c02.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:** These are the command parameters for this example:

8022B.0000.0c02.e649 = the IPX address of the BRI interface of the remote router. TIn 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 must 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 broadcast packets to be forwarded. Unless broadcast packets are specified as *interesting* packets by the **dialer-list** command, they are forwarded only when the ISDN link is active.

```
14155551234  
14155556789 = the remote router's ISDN telephone numbers.
```

```
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 by setting 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 service profile identifiers (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.

These are 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:** These are the command parameters for this example:

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

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

```
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:** These are the command parameters for this example :

301586E0 = the network portion of the remote server's internal IPX address. 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 remote router's BRI interface. 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:** These are 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 protocol ipx list 900
```

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

This is the remainder of the configuration:

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

## C4000 Configuration Explanation

The C4000 configuration is repeated, along with detailed explanations of many of the commands.

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

The username "C2503" 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 Challenge Handshake Authentication Protocol (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 a *Get Nearest Server* (GNS) request of a workstation to ensure the local file server can respond first.

```
isdn switch-type basic-5ess
```

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 8022C
```

8022C is 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 theaw 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.

The configuration continues:

```
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 Interior Gateway Routing Protocol/Enhanced Interior Gateway Routing Protocol (IGRP/EIGRP) routing metrics.

```
ipx network 8022B
```

8022B is 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 will remain active. A dialer map statement is required for each ISDN phone number that will be 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:** These are 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 must 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 forwarded only when the ISDN link is active.

```
14085554321
14085559876 = the remote router's ISDN telephone numbers.
```

```
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 login 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 by setting 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 service profile identifiers (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:** These are 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 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:** These are 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 remote server's console prompt 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:** These are 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:** These are 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 s**

2 = RIP hop count to the remote server

```
dialer-list 1 protocol ipx list 900
```

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

This is the remainder of the configuration:

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

# Troubleshooting ISDN Connectivity

1. Testing for physical connectivity and cabling problems.
2. Testing the SPIDs.
3. Testing for correct CHAP authentication.
4. Testing the call setup.

## Debugging Physical Connectivity

The `sh isdn status` command shows Layer 1 status as ACTIVE even when the link is not up.

```
c4000#sh isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
  Layer 1 Status:
    ACTIVE
  Layer 2 Status:
    TEI = 64, State = MULTIPLE_FRAME_ESTABLISHED
  Layer 3 Status:
    No Active Layer 3 Call(s)
  Activated dsl 0 CCBs = 0
  Total Allocated ISDN CCBs = 0
```

The `sh cont bri` command shows the ACTIVATED message for each of the D and B channels.

```
C4000#sh cont bri 0
BRI unit 0
D Chan Info:
Layer 1 is ACTIVATED
idb 0xB3B54, ds 0xC25A8, reset_mask 0x8
buffer size 1524
RX ring with 2 entries at 0x2101600 : Rxhead 0
00 pak=0x0C2E9C ds=0x4015AD8 status=D000 pak_size=0
01 pak=0x0C2938 ds=0x40146B0 status=F000 pak_size=0
TX ring with 2 entries at 0x2101640: tx_count = 0, tx_head = 0, tx_tail = 0
00 pak=0x000000 ds=0x000000 status=00 pak_size=0
01 pak=0x000000 ds=0x000000 status=00 pak_size=0
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
0 d channel collisions
B1 Chan Info:
Layer 1 is ACTIVATED
idb 0xB7E80, ds 0xC2680, reset_mask 0x0
buffer size 1524
RX ring with 8 entries at 0x2101400 : Rxhead 3
00 pak=0x0C3554 ds=0x4016F00 status=D000 pak_size=0
01 pak=0x0C4AE4 ds=0x401BFA0 status=D000 pak_size=0
02 pak=0x0C31BC ds=0x4016190 status=D000 pak_size=0
03 pak=0x0C474C ds=0x401B230 status=D000 pak_size=0
04 pak=0x0C4CB0 ds=0x401C658 status=D000 pak_size=0
05 pak=0x0C3720 ds=0x40175B8 status=D000 pak_size=0
06 pak=0x0C3388 ds=0x4016848 status=D000 pak_size=0
07 pak=0x0FDB04 ds=0x4053F28 status=F000 pak_size=0
TX ring with 2 entries at 0x2101440: tx_count = 0, tx_head = 1, tx_tail = 1
00 pak=0x000000 ds=0x000000 status=00 pak_size=0
01 pak=0x000000 ds=0x000000 status=00 pak_size=0
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
0 d channel collisions
B2 Chan Info:
```

```

Layer 1 is ACTIVATED
idb 0xBC1AC, ds 0xC2750, reset_mask 0x2
buffer size 1524
RX ring with 8 entries at 0x2101500 : Rxhead 0
00 pak=0x0C5534 ds=0x401E138 status=D000 pak_size=0
01 pak=0x0C5368 ds=0x401DA80 status=D000 pak_size=0
02 pak=0x0C519C ds=0x401D3C8 status=D000 pak_size=0

```

If the physical layer is not properly connected, the status is deactivated. This is an example:

```

C4000#sh cont bri 0
BRI unit 0
D Chan Info:
Layer 1 is DEACTIVATED
idb 0xB3B54, ds 0xC25A8, reset_mask 0x8
buffer size 1524
RX ring with 2 entries at 0x2101600 : Rxhead 0
00 pak=0x0C2E9C ds=0x4015AD8 status=D000 pak_size=0
01 pak=0x0C2938 ds=0x40146B0 status=F000 pak_size=0
TX ring with 2 entries at 0x2101640: tx_count = 0, tx_head = 0, tx_tail = 0
00 pak=0x000000 ds=0x000000 status=00 pak_size=0
01 pak=0x000000 ds=0x000000 status=00 pak_size=0
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
0 d channel collisions
B1 Chan Info:
Layer 1 is DEACTIVATED
idb 0xB7E80, ds 0xC2680, reset_mask 0x0
buffer size 1524

```

## Debugging SPIDS

Check if the TEI is assigned with a **sh isdn status** command. Layer 2 information shows if the TEI is assigned. Then, activate the **debug isdn events** and **debug isdn q931** commands. Finally, restart the interface with **clear int b 0**. The router sends its configured SPIDS to the ISDN switch and the switch either verifies them as correct or rejects them.

These are the commands that indicate if the SPIDS are correct:

```

C4000# debug isdn events
C4000# debug isdn q931
C4000# clear int b 0
BRI0: Physical layer DOWN
Activating ISDN line
BRI0: ISDN Event: incoming ces value = 1
BRI0: received HOST_TERM_REGISTER_NACK - invalid EID/SPID or TEI not
assigned
Cause i = 0x8082 - No route to specified network

```

For each SPID that is correct you see the received **HOST\_TERM\_REGISTER\_ACK** response from the switch. If you configure one SPID, you see only one acknowledge.

```

C4000#ping ipx 8022B.0000.0c09.509f

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 8022B.0000.0c09.509f, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/40/40 ms

%LINK-3-UPDOWN: Interface BRI0:1, changed state to up

```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to up
%ISDN-6-CONNECT: Interface BRI0:1 is now connected to 14085554321 c2500
```

This is the command to show an interface when a single B channel is active.

```
C4000#sh int b 0 1 2
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Closed: CDP
  Open: IPCP, IPXCP
  Last input 00:00:07, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/64/0 (size/threshold/drops)
    Conversations 0/1 (active/max active)
    Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    90 packets input, 2604 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    90 packets output, 2586 bytes, 0 underruns
    0 output errors, 0 collisions, 8 interface resets
    0 output buffer failures, 0 output buffers swapped out
    8 carrier transitions
```

Use the **sh isdn status** and **sh dialer** commands when the ISDN connection is up.

```
C4000#sh dialer
BRI0 - dialer type = ISDN

Dial String      Successes  Failures  Last called  Last status
14085554321      2          0         00:00:25    successful
14085559876      0          0         never       -
0 incoming call(s) have been screened.
BRI0:1 - dialer type = ISDN
Idle timer (300 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: ipx (s=8022B.0000.0c02.e649, d=8022B.0000.0c09.509f)
Time until disconnect 274 secs
Current call connected 00:00:27
Connected to 14085554321 (c2500)
BRI0:2 - dialer type = ISDN
Idle timer (300 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

C4000#sh isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
  Layer 1 Status:
    ACTIVE
  Layer 2 Status:
    TEI = 64, State = MULTIPLE_FRAME_ESTABLISHED
  Layer 3 Status:
    1 Active Layer 3 Call(s)
  Activated dsl 0 CCBs = 1
    CCB:callid=8002, sapi=0, ces=1, B-chan=1
  Total Allocated ISDN CCBs = 1
```

## Testing for CHAP Authentication

This is the output of the **debug ppp chap** command:

```
C4000#debug ppp chap
PPP authentication debugging is on
R2#ping ipx 100.0000.0c45.4211

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 8022B.0000.0c09.509f, timeout is 2 seconds:
.
%LINK-3-UPDOWN: Interface BRI0:1, changed state to up!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/42/44 ms
C4000#
PPP BRI0:1: Send CHAP challenge id=6 to remote
PPP BRI0:1: CHAP challenge from c2500
PPP BRI0:1: CHAP response received from c2500
PPP BRI0:1: CHAP response id=6 received from c2500
PPP BRI0:1: Send CHAP success id=6 to remote
PPP BRI0:1: remote passed CHAP authentication.
PPP BRI0:1: Passed CHAP authentication with remote.
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to up
%ISDN-6-CONNECT: Interface BRI0:1 is now connected to 14085554321 c2500
```

This is the debug output when CHAP authentication fails:

```
C4000#ping ipx 8022B.0000.0c09.509f

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 8022B.0000.0c09.509f, timeout is 2 seconds:
.
%LINK-3-UPDOWN: Interface BRI0:1, changed state to up
PPP BRI0:1: Send CHAP challenge id=7 to remote
PPP BRI0:1: CHAP challenge from c2500
PPP BRI0:1: CHAP response received from c2500
PPP BRI0:1: CHAP response id=7 received from c2500
PPP BRI0:1: Send CHAP failure id=7 to remote.
%LINK-3-UPDOWN: Interface BRI0:1, changed state to down
%LINK-3-UPDOWN: Interface BRI0:1, changed state to up
PPP BRI0:1: Send CHAP challenge id=8 to remote
PPP BRI0:1: CHAP challenge from c2500
PPP BRI0:1: CHAP response received from c2500
PPP BRI0:1: CHAP response id=8 received from c2500
PPP BRI0:1: Send CHAP failure id=8 to remote.
%LINK-3-UPDOWN: Interface BRI0:1, changed state to down
%LINK-3-UPDOWN: Interface BRI0:1, changed state to up
PPP BRI0:1: Send CHAP challenge id=9 to remote
PPP BRI0:1: CHAP challenge from c2500
PPP BRI0:1: CHAP response received from c2500
PPP BRI0:1: CHAP response id=9 received from c2500
PPP BRI0:1: Send CHAP failure id=9 to remote.
%LINK-3-UPDOWN: Interface BRI0:1, changed state to down
%LINK-3-UPDOWN: Interface BRI0:1, changed state to up
PPP BRI0:1: Send CHAP challenge id=10 to remote
PPP BRI0:1: CHAP challenge from c2500
PPP BRI0:1: CHAP response received from c2500
PPP BRI0:1: CHAP response id=10 received from c2500
PPP BRI0:1: Send CHAP failure id=10 to remote.
%LINK-3-UPDOWN: Interface BRI0:1, changed state to down
%LINK-3-UPDOWN: Interface BRI0:1, changed state to up
PPP BRI0:1: Send CHAP challenge id=11 to remote
PPP BRI0:1: CHAP challenge from c2500
PPP BRI0:1: CHAP response received from c2500
PPP BRI0:1: CHAP response id=11 received from c2500
```

```
PPP BRI0:1: Send CHAP failure id=11 to remote
Success rate is 0 percent (0/5)
%LINK-3-UPDOWN: Interface BRI0:1, changed state to down
```

## Call Setup Debug Messages

This output contains several debug commands used to check call setup.

```
C4000#debug isdn q931
ISDN Q931 packets debugging is on
C4000#debug isdn events
ISDN events debugging is on
R2#ping ipx 8022B.0000.0c09.509f

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 8022B.0000.0c09.509f, timeout is 2 seconds:
.
ISDN BR0: Event: Call to 14085554321 at 64 Kb/s
ISDN BR0: TX -> SETUP pd = 8 callref = 0x04
    Bearer Capability i = 0x8890
    Channel ID i = 0x83
    Keypad Facility i = 0x32333232303338
ISDN BR0: RX <- CALL_PROC pd = 8 callref = 0x84
    Channel ID i = 0x89
ISDN BR0: received HOST_PROCEEDING
    Channel ID i = 0x0101
    -----
    Channel ID i = 0x89
ISDN BR0: RX <- CONNECT pd = 8 callref = 0x84
ISDN BR0: received HOST_CONNECT
    Channel ID i = 0!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/40/40 ms
C4000#x0001
    -----
%LINK-3-UPDOWN: Interface BRI0:1, changed state to up
ISDN BR0: Event: Connected to 14085554321 on B1 at 64 Kb/s
ISDN BR0: TX -> CONNECT_ACK pd = 8 callref = 0x04
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to up
%ISDN-6-CONNECT: Interface BRI0:1 is now connected to 14085554321 c2500
```

In a successful ISDN call, the Bearer Capability (BC) sent from the router that initiates the call also is received at the end that answers the call. It is possible to order ISDN services with many different types of services, such as voice only, 56KB data, and 64KB data.

Bearer Capability	Description
0x8890	64KB/sec data call
0x8890218f	56KB/sec data call
0x8090A2	Voice call

---

## Related Information

- [Novell NetWare in DDR Environments](#)
  - [LAN Technologies Technical Tips](#)
  - [Technical Support & Documentation – Cisco Systems](#)
-

