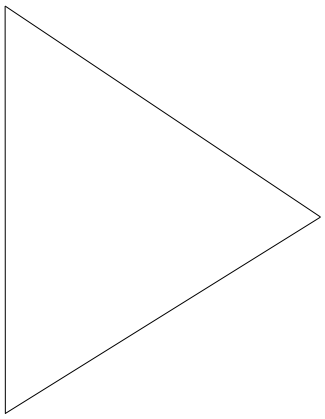
Design and Implementation Guide Addendum

Jeff Baher
jbaher@cisco.com
Technical Marketing



December 1995

Integrated Services Digital Network (ISDN)

Overview

Like many of today's technologies, Integrated Services Digital Network (ISDN) is rapidly growing and changing. As a result of these changes, Cisco is constantly refining both its product offerings and its software features.

Most notable is the acquisition of Combinet, Inc. which helps to expand Cisco's low-end ISDN product offerings. The first wave of new products comprise the 750 series, a new line of low-end ISDN solutions for homes and small offices.

Cisco has also released a set of new software features as part of Release 11.0 (3) of the Cisco Internetwork Operating System (Cisco IOS™) software. These features are designed to make more efficient and effective use of ISDN services with Cisco products.

This addendum is intended to address the new additions to the Cisco product line as well as provide in-depth coverage of the latest ISDN-related Cisco IOS features.

The Combinet Acquisition

Cisco's acquisition of Combinet, Inc., extends Cisco's ISDN offerings to small offices, home offices, and individual users.

The Combinet products give Cisco an instant presence in the fast-growing telecommuting market. In particular, the Combinet 2000 series brings to Cisco a family of low-cost, entry-level ISDN products that support IP and IPX routing, bridging, Simple Network Management Protocol (SNMP) management, and multilevel security. Combinet currently has a 27 percent share of the U.S. telecommuting market, and its products are available in over 20 countries.

In addition to the 2000 series, the Combinet product line includes a family of ISA bus PC adapter cards, an ISDN primary rate interface (PRI) product for central site applications, and Connection Manager, a Windows-based call management, device configuration, and accounting application.

Versions of the Combinet 2000 series products were introduced into the Cisco and CiscoPro™ product lines beginning in November of 1995. Enterprise products will be known as the Cisco 750 series, and products intended for the two-tier channel will be known as the CiscoPro 750 series.

Product Positioning: Cisco 750 and Cisco 1000

The Cisco 750 series provides an ISDN access solution that is complementary to the Cisco 1000 family. While the Cisco 1000 series is ideal for branch office connectivity, the Cisco 750 series is targeted toward telecommuters, professional offices, and home offices that need IP and IPX routing functionality over ISDN.

CISCO SYSTEMS

The Cisco 750 series represents the lowest-cost entry point into the Cisco family of access routers, and provides an optional analog basic telephone service (POTS) interface (model 753) to reduce the overall cost of the telecommuting solution. The ConnectPro software provides a Windows-based graphical user interface that simplifies the process of installing, configuring, and managing Cisco 750 series products.

The standard version of the Cisco 750 series supports up to four devices on the directly attached LAN. A software upgrade option is available for users who require support for more than four devices on the local LAN.

The Cisco 1000 series is targeted at remote offices and branch offices. It features IP, IPX, and AppleTalk routing, as well as advanced routing protocols such as Enhanced IGRP® and Snapshot Routing. The Cisco 1000 series also supports Priority Queuing and Custom Queuing to optimize WAN bandwidth utilization.

A feature comparison of the Cisco 750 and Cisco 1000 products follows.

Table 1.

Cisco 750	Cisco 1000
Telecommuter, home office professional office	Branch office, remote office
IP and IPX routing	IP, IPX, and AppleTalk routing
Low cost	Enhanced IGRP
ConnectPro and personal network profiles	Optional Flash ROM
Optional POTS integration	PCMCIA card
Up to four LAN devices (standard version) $999-$1799 U.S. list	No restriction on LAN devices $1395-$2195 U.S. list

Additional positioning materials are currently being developed and will be available by the Cisco 750 series launch date.

The Combinet Product Line

While not all Combinet products have been integrated into the Cisco product line, the following is a brief overview of ConnectProCombinet's complete product offerings.

Table 2.

Product	Description	Target Market	List Price
PC-1000	PC ISA card BRI	Telecommuting, single-user Internet access	$499–$799
CB-2000	Ethernet/BRI IP/IPX router	Telecommuting, professional office, Internet	$999–$1699
CB-900	Ethernet/PRI IP/IPX router	Telecommuting, regional office	$4990
ConnectionManager	Windows-based remote access management application		$895
ConnectPro	Windows-based GUI configuration tool		N/C

The CB-2000 products are available in the following four versions:

Table 3.

Product	Description	List Price
CB-2050B	ISDN router—four network devices	$999

Table 3.

CB-2050D	ISDN router—unrestricted devices	$1499
CB-2060A	ISDN router with NT1—four network devices	$1199
CB-2060D	ISDN router with NT1—unrestricted devices	$1699

The Combinet 2050B will be introduced in the Cisco enterprise product line as the Cisco 751, and the 2060A will become the Cisco 752. Features and functionality of the Cisco and CiscoPro versions will be differentiated over time.

The Cisco 753 is a new product that includes a basic telephone service interface and a built-in Network Termination 1 (NT1). The telephone service interface allows a standard analog telephone, fax machine, or modem to share the ISDN BRI line with data traffic. This product will have a list price of $1399 for the standard four-device version.

The Cisco 750 series is orderable now and began shipping on November 15. The CiscoPro 750 series is also orderable now and began shipping to Ingram Micro and Tech Data during the first week in November.

Cisco 750 Series Configuration

Use of Profiles

The 75X products provide for varying profiles, which are a set of configurations customized for and associated with a specific remote device. Once defined by the user, profiles are stored and saved in NVRAM.

The profile types supported are as follows:

- *Permanent:* Can be modified but not deleted.
  - *LAN:* Determines how data is passed from a router to the LAN.
  - *Standard:* Used for incoming ISDN connections that do not have profiles; does *not* support routing. It should be used to provide the appropriate configuration and security measures for unknown callers.
  - *Internal:* Determines how data is passed between the bridge engine and the IP/IPX router.
- *User:* Set up for each individual user/remote site; up to 17 profiles can be configured in 750 series units. Note: Due to memory limitations and depending on the complexity of the profiles, 17 profiles may be unattainable. Remember, however, that these products are intended for the house and small office so in all likelihood this won't be a problem.

Profile Parameters

Profile parameters can be configured on a per-profile basis and apply solely to the specific profile. Any configuration changes to profile parameters while in profile mode apply only to that profile. The following are all profile parameters:

- Auto Calling
- Bridge Type Filters
- Bridging
- Callback
- Callback ID Security
- Callback Receive Numbers
- Called Number
- CHAP Host Secret
- Compression

- Demand Parameters
- Encapsulation
- IP Parameters
- IPX Parameters
- Learning
- Line Speed
- Loopback
- PAP Host Password
- Passwords
- PPP Authentication Outgoing
- Protocol
- Ringback Number

System Parameters

System parameters are independent of profiles and affect the router as a system. System parameters can be changed only at the system-level prompt. If modified while in profile mode, they will apply to all profiles. The following are all system parameters:

- Caller ID Parameters
- Date and Time
- Delay Times
- Directory Number
- Forwarding Mode
- Multidestination
- Numbering Plan
- Passthru
- Patterns
- PPP Parameters
- PS 1 Detect
- Screen Echo
- Screen Length
- SNMP Parameters
- System Passwords

Changing any profile parameters at the system level changes the values for the profile template.

To simplify configuring a multitude of profiles, a profile template can be configured at the system level to configure the same profile parameters throughout all profiles. Any profile that has a specific profile parameter redefined within the profile is not affected by a change to the profile template configuration.

Basic Setup

After a Cisco 750 series unit is cabled and powered on, ensure that the “Line” and “NT1” LEDs are illuminated. This will verify that the ISDN line and built-in NT1 are functioning. This should be followed by the **show config** command to verify current ISDN-specific settings.

The following commands need to be entered at the system level to configure ISDN parameters to adhere to a site’s specific ISDN setup:

```
set switch [type]              (default is 5ess) Refer to documentation for ISDN switch support
set directory [number]         (directory number assigned by local telephone company)
set SPID [spid-number]         (number identifying service to which you have subscribed)
```

To test the ISDN connection, change to profile mode (cd test) and place a call from one B channel to a second one with the following command:

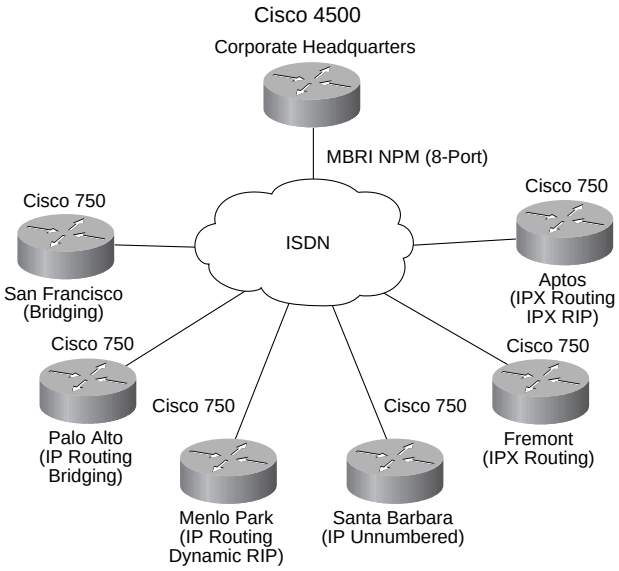
```
call [channel]                 [phone number]
```

The channel is either B1 or B2, and the number is the phone number associated with the BRI interface. Once this is working, you can be assured that the local site has its ISDN line ready for configurations to the remote site.

Sample Configurations

The following section shows sample configurations for the network depicted in Figure 1. The Cisco 4500 BRI router is acting as a branch office router connecting multiple incoming telecommuters from around the area who are using Cisco 75X routers.

Figure 1. Cisco 750/Cisco IOS Network Design Scenarios



A Brief Note About the Cisco 75X User Interface

For UNIX and DOS users, the Cisco 75X user interface will be familiar ground. The Cisco 75X interface is command-line driven and uses the concept of a root directory and subdirectories to configure parameters. The root directory or system level is represented using the “>” symbol. If the “set system name” command is used to assign a name to the device, the root prompt will change to reflect this. For example, “set system name jackstraw” will change the root prompt to “jackstraw>.”

The subdirectories come into play when configuring profiles. To configure the LAN profile, or a user profile, you must navigate to the respective subdirectory. Navigating subdirectories is done by using the “CD” command, just like UNIX or DOS. Typing “CD LAN” will move you to the LAN profile. The prompt will change to “:LAN>” to reflect this move. For user profiles, the “set user <user profile name>” command will automatically move you into the newly created user profile subdirectory. For example “jackstraw> set user stellablue” will automatically put you in the “:stellablue>” subdirectory. The command “CD” will return you to the system level.

It is also important to note that commands need not be input in full in order for them to be accepted. For example, to enter a system name the “set system name <system name>” command can be abbreviated as follows: SE SY <system name>.” The best place to go to familiarize yourself with the Cisco 75X abbreviated commands is the Cisco 75X manual. The manual is extremely useful from this standpoint as well as for learning more about the units and all of the different command options.

The section that follows provides a variety of different configurations for connecting Cisco 75X units to Cisco IOS-based units. The Cisco 75X syntax provided is intended to illustrate the requisite commands. The configurations, however, do not show the prompt and therefore do not reflect directory changes.

Special thanks to Art Howarth for his work in developing these configurations.

Configuring Bridging Profiles

Use the following configuration for the Cisco 75X router in San Francisco, which only needs to bridge.

Command	Function
`set system sanfrancisco`	`:system name cannot exceed 16 characters`
`set wan mode any`	`:enable bridging unknown packets to the WAN`
`set user sanjose`	`:creates profile named San Jose - profiles can be up to 20 characters long`
`set encapsulation ppp`	
`set number 5551212`	`:remote router’s ISDN number`
`cd`	`:return to root prompt`
`reboot`	`:enables modifications`

The corresponding configuration on the Cisco 4500 using bri0 to communicate with the router in San Francisco is as follows:

Command	Function
`hostname sanjose`	
`!`	
`username sanfrancisco`	
`no ip routing`	`:disables IP routing`
`isdn switch-type basic-5ess`	
`!`	
`interface Ethernet0`	

Command	Function
no ip address	
no mop enabled	
bridge-group 1	:enables bridging for interface
no shutdown	
!	
interface BRI0	
no ip address	
encapsulation ppp	
dialer map bridge name sanfrancisco 5551414	
no ip route-cache	
dialer-group 1	
bridge-group 1	:enables bridging for interface
bridge-group 1 spanning-disabled	:disables BPDU transmissions
no shutdown	
!	
!	
dialer-list 1 protocol bridge permit	
bridge 1 multicast-source	:permits the forwarding of multicast frames
bridge 1 protocol ieee	:enables IEEE bridging

Configuring IP Routing Profiles

IP Static Routing

The following configuration is used for the Cisco 75X router in Palo Alto, which needs to route IP. A default static route is used to get to the branch office and beyond.

Command	Function
set system paloalto	
cd lan	
set ip address 150.150.150.1	:ip address for local Ethernet
set ip netmask 255.255.255.0	
set ip routing on	
set ip rip update periodic	:enables periodic RIP updates (every 30 sec.)
cd	
set user sanjose	

Command	Function
`set ip address 150.150.151.2`	:ip address for local BRI interface
`set ip netmask 255.255.255.0`	
`set ip routing on`	:enables IP routing
`set ip framing none`	:enables IPCP
`set ip rip update off`	:disables RIP on this profile
`set encapsulation ppp`	
`set ip route destination 200.200.200.0/24 gateway 150.150.151.1 pr=on`	:static route entry; “pr=on” propagates the static route
`set number 5551212`	
`set timeout=30`	:idle timeout value
`set bridging=off`	
`cd reboot`	

The corresponding Cisco 4500 configuration is as follows:

Command	Function
`hostname sanjose`	
`!`	
`username paloalto`	
`ip routing`	
`isdn switch-type basic-5ess`	
`!`	
`interface Ethernet0`	
`ip address 200.200.200.1 255.255.255.0`	
`no shutdown`	
`!`	
`interface BRI0`	
`ip address 150.150.151.1 255.255.255.0`	
`encapsulation ppp`	
`dialer map ip 150.150.151.2 name paloalto 5551414`	:dialer map pointing to the Cisco 750’s BRI interface
`no ip route-cache`	
`dialer-group 1`	
`no shutdown`	
`!`	
`router rip`	

Command	Function
redistribute static	
passive interface b 0	:disables RIP updates on the int b 0
network 200.200.200.0	
redistribute connected	
ip route 150.150.150.0 255.255.255.0 150.150.151.2	:static route to the Cisco 750’s Ethernet
dialer-list 1 protocol ip permit	:permits IP packets over the ISDN link

IP Dynamic Routing

Use the following configuration for the Cisco 75X router in Menlo Park, which needs to route IP. RIP is used as the dynamic IP routing protocol. Bridging is disabled in this example.

Command	Function
set system menlopark	
cd lan	
set ip address 150.150.150.1	
set ip netmask 255.255.255.0	
set ip routing on	
set ip rip update periodic	
cd	
set user sanjose	
set ip address 150.150.151.2	
set ip netmask 255.255.255.0	
set ip routing on	
set ip rip update periodic	:enables RIP on this profile
set encapsulation ppp	
set ip framing none	
set number 5551212	
set bridging=off	:disables bridging on this profile
cd	
reboot	

The corresponding Cisco 4500 configuration is as follows:

Command	Function
hostname sanjose	
!	

Command	Function

```
username menlopark

isdn switch-type basic-5ess

!

interface Ethernet0

ip address 200.200.200.1 255.255.255.0

no mop enabled

no shutdown

!

interface BRI0

ip address 150.150.151.1 255.255.255.0

encapsulation ppp

dialer map ip 150.150.151.2 name menlopark
  5551414

dialer-group 1

no shutdown

!

router rip

network 200.200.200.0

network 150.150.150.0

!

!

dialer-list 1 protocol ip permit
```

IP Unnumbered

An IP connection may be unnumbered only if *all* of the following are true:

- The connection is a WAN connection (not the internal or LAN connection) to a router or single node
- PPP IPCP encapsulation is being used (framing is set to NONE)
- Static routes, and *not* periodic or demand RIP, are being used to establish routes to the connection.

An IP connection can be made unnumbered by setting its IP address to 0.0.0.0. Static routes should be created for unnumbered connections by issuing a set ip route field in the connection's profile. The gateway field in the **set up route** command should be set to 0.0.0.0.

Example:

```
set ip framing none
set ip address 0.0.0.0
set ip rip update off
set ip rip receive off
set ip route dest 144.172.17.0/24 gateway 0.0.0.0
set ip routing on
```

To configure a Cisco 75X router in Santa Barbara using IP unnumbered, use the following:

Command	Function
`set system santabarbara`	
`cd lan`	
`set ip address 150.150.150.1`	
`set ip netmask 255.255.255.0`	
`set ip routing on`	
`set ip rip update periodic`	
`cd`	
`set user sanjose`	
`set ip routing on`	`:enables IPCP on this profile`
`set ip framing none`	
`set ip rip update off`	`:disables RIP updates`
`set encapsulation ppp`	
`set ip route destination 0.0.0.0 ga 0.0.0.0`	
`set number 5551212`	
`set timeout=30`	
`set bridging=off`	`:disables bridging on this profile`
`cd`	
`reboot`	

The corresponding Cisco 4500 configuration is as follows:

Command	Function
`hostname sanjose`	
`!`	
`username santabarbara`	
`isdn switch-type basic-5ess`	
`!`	
`interface Ethernet0`	
`ip address 200.200.200.1 255.255.255.0`	
`no mop enabled`	
`no shutdown`	
`!`	
`interface BRI0`	
`ip unnumbered Ethernet0`	

Command	Function
encapsulation ppp	
dialer map ip 150.150.150.1 name santabarbara 5551414	
dialer-group 1	
no shutdown	
!	
router rip	
redistribute static	
passive interface b 0	
network 200.200.200.0	
!	
ip route 150.150.150.0 255.255.0.0 BRI0	
!	
access-list 101 permit ip any any	
!	
dialer-list 1 list 101	

Configuring IPX Routing Profiles

Note: Combinet does not support the IPX/SPX default gateway.

IPX Static Routing

The following configuration is for a Cisco 75X router in Fremont that routes IPX. A static route is used back to corporate headquarters. The Cisco 750 series supports up to 15 static IPX routes.

Command	Function
set system fremont	
set user sanjose	
cd sanjose	
set ipx network 100	
set ipx routing on	
set ipx rip update off	
set encapsulation ppp	
set ipx framing none	:enables IPXCP framing
set number 5551212	
set timeout=30	

Command	Function
`set ipx route destination=200 gateway=100:0000c6067f5a`	`:static route to Cisco 4500's Ethernet`
`set ipx route destination=3039e670 gateway=100:0000c6067f5a`	`:static route to NetWare server's internal network`
`set ipx server name corp_fs1 ty 4 address 3039e670:01:0451`	`:static IPX SAP entry`
`set bridging=off`	
`cd`	
`cd lan`	
`set ipx network 150`	
`set ipx framing 802.2`	
`set ipx routing on`	
`set ipx rip update periodic`	
`cd`	
`reboot`	

The corresponding Cisco 4500 configuration is as follows:

Command	Function
`hostname sanjose`	
`!`	
`username fremont`	
`!`	
`no ip routing`	
`ipx routing 0000.0c3b.c743`	
`isdn switch-type basic-5ess`	
`!`	
`interface Ethernet0`	
`ipx network 200`	
`ipx encapsulation sap`	
`no mop enabled`	
`no shutdown`	
`!`	
`interface BRI0`	
`encapsulation ppp`	
`ipx network 100`	

Command	Function
`dialer map ipx 100.0040.f902.c7b4 name fremont 5551414`	
`no shutdown`	
`!`	
`ipx route 150 100.0040.f902.c7b4`	
`!`	
`ipx router rip`	
`no network 100`	
`!`	
`dialer-list 1 protocol ipx permit`	

IPX Dynamic Routing

The following configuration is for a Cisco 75X router in Aptos that routes IPX and wants to use periodic RIP updates:

Command	Function
`set system aptos`	
`set user sanjose`	
`cd sanjose`	
`set ipx network 100`	
`set ipx routing on`	
`set ipx rip update periodic`	
`set ipx framing none`	
`set encapsulation ppp`	
`set number 5551212`	
`set timeout=30`	
`set br=off`	
`cd`	
`cd lan`	
`set ipx network 150`	
`set ipx fr 802.2`	
`set ipx routing on`	
`set ipx rip update periodic`	
`cd`	
`reboot`	

The corresponding Cisco 4500 configuration is as follows:

Command	Function

```
hostname sanjose
!
username aptos
!
no ip routing
ipx routing 0000.0c3b.c743
isdn switch-type basic-5ess
!
interface Ethernet0
ipx network 200
ipx encapsulation sap
no mop enabled
no shutdown
!
interface BRI0
encapsulation ppp
ipx network 100
dialer map ipx 100.0040.f902.c7b4 name aptos
  5551414
dialer-group 1
no shutdown
!
!
dialer-list 1 protocol novell permit
```

Advanced Configurations

The Cisco 75X routers also support the following advanced features:

- PAP/CHAP
- Filtering
- CallerID
- Callback
- Point-to-Point Protocol (PPP) Multilink
- Debugging

PAP/CHAP

The Cisco 75X supports both PPP CHAP and PAP authentication. The Cisco 75X uses the keyword “password” for PAP authentication and the keyword “secret” for CHAP authentication. The CHAP/PAP secret/password is limited to 16 characters. PPP will always send the system name as the user identification. While either CHAP or PAP can be used for authentication between a Cisco 75X and a Cisco IOS-based unit, CHAP is recommended because of its greater security. In order for CHAP to work, the following must be configured:

• 750 system name == Cisco username	`The Cisco 75X system name must be entered as a username on the Cisco IOS device`
• 750 profile name == Cisco hostname	`A profile must be created on the 75X that has the same name as the Cisco IOS hostname`
• 750 Chap Host secret == Cisco Username Secret	`The 75X secret must be the same as the Cisco IOS username password`
• 750 Chap Client secret == Cisco Username Secret	`The 75X secret must be the same as the Cisco IOS username password`

The 75X uses four principals’ commands to address PPP authentication.

- Host Password—The host password is used during PAP authentication when the unit is the authenticator. The remote device sends its client password to this unit. (If the client’s password matches the authenticator’s host password, the call is allowed.) **The host password is a profile-based command.**
- Client Password—The client password is used during PAP authentication when this unit is the device authenticated. This unit sends its client password to the authenticator. If the client password matches the authenticator’s host password, the call is allowed. **The client password is a system level parameter.**
- Host Secret—The host secret is used during CHAP authentication when this unit is the authenticator. This unit sends a challenge to the remote device in the form of a random number. The remote device uses its client secret to perform a calculation on the number. This unit uses its host secret to perform a calculation on the same number. If the answers to both calculations match, the call is allowed. **The host secret is a profile-based command.**
- Client Secret—A client secret is used during CHAP authentication when this unit is the device being authenticated. The authenticator sends this unit a challenge in the form of a random number. This unit uses its client secret to perform a calculation on the number. The authenticator uses its host secret to perform a calculation on the same number. If the answers to both calculations match, the call is allowed. **The client secret is a system level parameter.**

A 75X unit can have one host password/secret per profile, and one client password/secret per unit.

The following configuration is for a Cisco 75X router with PAP authentication:

Command	**Function**
`set system 2060`	
`cd lan`	
`set ip address 150.150.150.1`	
`set ip netmask 255.255.255.0`	
`set ip routing on`	
`set ip rip update period`	
`cd`	
`set user 2503`	
`set ip address100.100.100.2`	
`set ip netmask 255.255.255.0`	

Command	Function
set ip routing on	
set ip framing none	
set encapsulation ppp	
set ip route destination 200.200.200.0/24 ga 100.100.100.1 pr=on	
set number 5551212	
set bridging=off	
set timeout=30	
cd	
set ppp authentication in pap	:sets ppp auth. for incoming packets
set ppp authentication out pap	:sets ppp auth. for outgoing packets
set ppp password client	:sets ppp password
cisco	:password must be input twice for verification
cisco	:password must be input twice for verification
cd 2503	
set ppp password host	:configures host ppp password
cisco	:password must be input twice for verification
cisco	:password must be input twice for verification
reboot	

The corresponding Cisco 4500 configuration is as follows:

Command	Function
hostname 2503	
!	
username 2060 password cisco	:password will be displayed in encrypted form
username 2503 password cisco	
isdn switch-type basic-5ess	
!	
interface Ethernet0	
ip address 200.200.200.1 255.255.255.0	
no mop enabled	
no shutdown	
!	
interface BRI0	
ip address 100.100.100.1 255.255.255.0	

Command	Function
encapsulation ppp	
ppp authentication pap	
dialer map ip 100.100.100.2 name 2060 5551414	
dialer-group 1	
no shutdown	
!	
router rip	
redistribute static	
network 200.200.200.0	
redistribute connected	
!	
ip route 150.150.150.0 255.255.255.0 100.100.100.2	
!	
dialer-list 1 protocol ip permit	

The following configuration is for a Cisco 75X router with CHAP authentication:

Command	Function
set system 2060	
cd lan	
set ip address 150.150.150.1	
set ip netmask 255.255.255.0	
set ip routing on	
set ip rip update periodic	
cd	
set user 2503	
set ip address100.100.100.2	
set ip ne 255.255.255.0	
set ip routing on	
set ip framing none	
set encapsulation ppp	
set ip route destination 200.200.200.0/24 ga 100.100.100.1 pr=on	
set number 5551212	
set bridging=off	

Command	Function
set timeout=30	
cd	
set ppp authentication in chap	
set ppp authentication out chap	
set ppp secret client	
cisco	
cisco	
cd 2503	
set ppp secret host	
cisco	
cisco	
set bridging=off	
reboot	

The corresponding Cisco 4500 configuration is as follows:

Command	Function
hostname 2503	
!	
username 2060 password cisco	
isdn switch-type basic-5ess	
!	
interface Ethernet0	
ip address 200.200.200.1 255.255.255.0	
no mop enabled	
no shutdown	
!	
interface BRI0	
ip address 100.100.100.1 255.255.255.0	
encapsulation ppp	
ppp authentication chap	
dialer map ip 100.100.100.2 name 2060 5551414	
dialer-group 1	
no shutdown	
!	

Command	Function
`router rip`	
`redistribute static`	
`network 200.200.200.0`	
`redistribute connected`	
`!`	
`ip route 150.150.0.0 255.255.0.0 100.100.100.2`	
`!`	
`dialer-list 1 protocol ip permit`	

Filtering

The following filtering capabilities are available with the Cisco 750 series:

- IP filters:
- TCP, UDP, ICMP
- Various TCP and UDP ports
- All addresses, nets of addresses, and single addresses
- Blocking or accepting traffic
- Implicit deny-all like Cisco

IPX Filters

User will have to know how the hex values of the protocol if filtering is to be done.

[no filtering for IPX except for serialization packets]

Filtering Example

Command	Function

```
set system 2060

cd lan

set ip address 150.150.150.1

set ip netmast 255.255.255.0

set ip routing on

set ip rip update periodic

cd

set user 2503

set ip address 100.100.100.2

set ip netmask 255.255.255.0

set ip routing on

set ip framing none

set encapsulation ppp

set ip route destination 200.200.200.0/24

  ga 100.100.100.1 pr=on

set number 5551414

set bridging=off

set timeout 30

cd

cd 2503

set ip filter tcp in destination=0.0.0.0:23
  block

set ip filter tcp in destination=0.0.0.0:513
  block

set ip filter tcp in destination=0.0.0.0:514
  block

set ip filter tcp in destination=0.0.0.0:21
  block

set ip filter tcp out destination=0.0.0.0:21
  block

set ip filter udp in destination=0.0.0.0:69
  block

set ip filter udp out destination=0.0.0.0:69
  block

cd

set bridging=off
```

Command	Function
reboot	

CallerID

Use the CallerID feature to filter dial-in access based on an incoming ISDN phone number:

Command	Function
set system menlopark	
cd lan	
set ip address 150.150.150.1	
set ip netmask 255.255.255.0	
set ip routing on	
set ip rip update periodic	
cd	
set user sanjose	
set ip address 100.100.100.2	
set ip netmask 255.255.255.0	
set ip routing on	
set ip rip update periodic	
set encapsulation ppp	
set ip framing none	
set number 5551212	
set bridging=off	
cd	
set callerid on	:enables callerID
set callid 5551212	:maps callerID to incoming ISDN number
reboot	

The corresponding Cisco 4500 configuration is as follows:

Command	Function
hostname sanjose	
!	
username menlopark	
isdn switch-type basic-5ess	
!	
interface Ethernet0	

Command	Function
`ip address 200.200.200.1 255.255.255.0`	
`no mop enabled`	
`no shutdown`	
`!`	
`interface BRI0`	
`ip address 100.100.100.2 255.0.0.0`	
`encapsulation ppp`	
`dialer map ip 150.150.150.1 name menlopark 5551414`	
`dialer-group 1`	
`isdn caller 5551414`	`:maps callerID to ISDN number`
`no shutdown`	
`!`	
`router rip`	
`network 200.200.200.0`	
`network 100.100.100.0`	
`!`	
`!`	
`dialer-list 1 protocol ip permit`	

PPP Callback

Use PPP Callback to enable callback to sites attempting to dial in:

Command	Function
`set system menlopark`	
`cd lan`	
`set ip address 150.150.150.1`	
`set ip netmask 255.255.255.0`	
`set ip routing on`	
`set ip rip update periodic`	
`cd`	
`set user sanjose`	
`set ip address 100.100.100.2`	
`set ip netmask 255.255.255.0`	
`set ip routing on`	
`set ip framing none`	

Command	Function
set ip rip update periodic	
set encapsulation ppp	
set ppp callback request always	:establishes a callback request. The “always” keyword forces the calling unit to disconnect after negotiation.
set number 5551212	
set bridging=off	
cd	
reboot	

The corresponding Cisco 4500 configuration is as follows:

Command	Function
hostname sanjose	
!	
username menlopark	
isdn switch-type basic-5ess	
!	
map-class dialer bri0	:configures a dialer map class for PPP callback
dialer callback-server username	:specifies whether the dialstring to call is to be identified by looking up the authenticated hostname or is determined during callback negotiation
!	
!	
!	
interface Ethernet0	
ip address 200.200.200.1 255.255.255.0	
no mop enabled	
no shutdown	
!	
interface BRI0	
ip address 100.100.100.2 255.0.0.0	
encapsulation ppp	
ppp callback accept	:configures the interface to accept PPP callback
dialer map ip 150.150.150.1 name menlopark class bri0 5551414	:use class command to map to a defined map-class
dialer-group 1	

Command	Function
ppp authentication chap	
dialer hold-queue 10 timeout 15	:allows queuing of packets while link comes up
dialer enable-timeout 1	:allows the interface to be re-enabled after only 1 second
no shutdown	
!	
router rip	
network 200.200.200.0	
network 100.100.100.0	
!	
!	
dialer-list 1 protocol ip permit	

PPP Multilink

PPP Multilink is enabled by default on the Cisco 750 series and disabled by default on Cisco IOS platforms. Below are PPP Multilink configurations for Cisco 750 and Cisco IOS platforms:

Command	Function
set system menlopark	
cd lan	
set ip address 150.150.150.1	
set ip netmask 255.255.255.0	
set ip routing on	
set ip rip update periodic	
cd	
set user sanjose	
set ip address 100.100.100.2	
set ip netmask 255.255.255.0	
set ip routing on	
set ip framing none	
set ip rip update periodic	
set encapsulation ppp	
set number 5551212	
set bridging=off	
cd	
reboot	

The corresponding Cisco 4500 configuration is as follows:

Command	Function
`hostname sanjose`	
`!`	
`username menlopark`	
`isdn switch-type basic-5ess`	
`!`	
`interface Ethernet0`	
`ip address 200.200.200.1 255.255.255.0`	
`no mop enabled`	
`no shutdown`	
`!`	
`interface BRI0`	
`ip address 100.100.100.2 255.0.0.0`	
`encapsulation ppp`	
`dialer map ip 150.150.150.1 name menlopark 5551414`	
`ppp multilink`	`:enables PPP Multilink`
`dialer load-threshold 50 either`	`:enables B-channel aggregation regardless of traffic direction`
`dialer-group 1`	
`no shutdown`	
`!`	
`router rip`	
`network 200.200.200.0`	
`network 100.100.100.0`	
`!`	
`!`	
`dialer-list 1 protocol ip permit`	

Debugging

The following command can be used on Cisco 75X routers to perform debugging: **log n traffic verbose**

where n is the connection number (only required when you want to specify a connection corresponding to other than the current profile).

You can add the optional keywords INCOMING or OUTGOING to log packets in the specified direction only.

The **log packets** command gives traffic statistics for the specified connection once per second. There is no verbose option for log packets.

For more information on the log command, refer to the Cisco 75X documentation.

Interoperability Issues

Bridging right now does *not* operate if the Cisco 75X Combinet product calls the Cisco router; it only operates when the Cisco router calls the Combinet product.

The default ISDN packet encapsulation protocol is Combinet Packet Protocol (CPP). If you are connecting to a Cisco IOS router, you must change the encapsulation to PPP with the **set encapsulation ppp** command.

The Cisco 750 series implements Multilink PPP (RFC 1717). Multilink PPP is available in Cisco IOS Versions 11.0(3) and later. If you are connecting a Cisco 750 series to a Cisco IOS router running a Cisco IOS version prior to 11.0(3), you must disable multilink PPP with the **set ppp multilink off** command.

When configuring the Cisco 750 series for IP and/or IPX routing to a Cisco IOS router, the Cisco 750 must be configured for Internet Protocol Control Protocol (IPCP) and/or Internetwork Packet eXchange Control Protocol (IPXCP). In the Cisco 750 remote profile, use the **set ip framing none** and/or **set ipx framing none** commands. Do not use these values in the LAN profile.

The Cisco 750 series implements RIP version 2 (RFC 1723) and Demand RIP (RFC 1582). These proposed standards are not implemented in the Cisco IOS software. If you are connecting to a Cisco IOS router and want to use a dynamic routing protocol, you must configure the Cisco 750 for RIP version 1 using the **set IP RIP version 1** command and disable demand RIP with the **set ip rip update periodic** command.

The Cisco 750 series implements compression only over the CPP protocol. This is not compatible with the Cisco IOS software as mentioned above.

Cisco IOS routers can only bridge to a single remote site at a time over ISDN. IP and IPX routing do not have this restriction.

For more information on the Cisco 750 series, refer to the Cisco 750 series documentation.

Cisco IOS 11.0 (3) Features

In addition to the Cisco 750 series, the Cisco IOS software has also gained increased ISDN functionality. Below is a discussion of the principal ISDN features available in Cisco IOS Release 11.0(3) and later:

PPP Multilink for ISDN Interfaces

(Refer to the “Cisco 750 Configuration” section for an example of PPP Multilink for ISDN on Cisco IOS platforms.)

Description

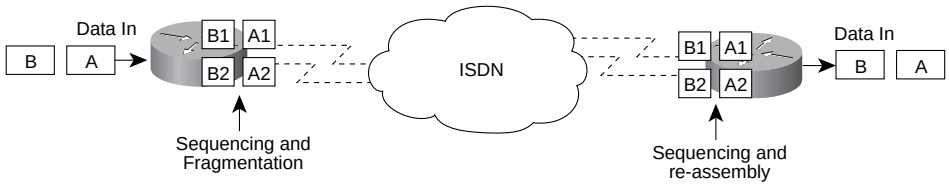
PPP Multilink (MP) is a method of B-channel aggregation that is defined in Internet Engineering Task Force (IETF) RFC 1717. This RFC defines a means by which packets can be sequenced and transmitted over multiple physical interfaces. To reduce potential latency issues, MP also defines a method of fragmenting and reassembling large packets.

MP is supported and can be used with any Cisco ISDN BRI or PRI interface. MP can be used in conjunction with other ISDN features including PPP Compression (CCP), PPP Authentication, PPP Callback, and IP Address Negotiation.

It is important to note that MP does *not* define how or why B-channel links should be initiated or torn down. The design of this mechanism has been left to the vendors. Cisco’s implementation allows the user to define a loading factor (the percentage of bandwidth being used on a B channel, at which point a second or subsequent B channel call should be initiated. This loading factor can be defined for only incoming, only outgoing, or either incoming or outgoing load. This allows MP to be used effectively in many different environments, such as collecting information from the Internet/WWW (mostly incoming traffic) or sending files to colleagues (mostly outgoing traffic).

Figure 2 illustrates a basic MP session. Here a second B channel is already in use and MP is in operation. Incoming packets A and B are both fragmented into smaller packets. These are then given sequence numbers by MP and shared over the two B channels. Note that all packets greater than 30 bytes are subject to fragmentation. When the fragments of packet A and B arrive at the receiving router, MP reassembles the original packets and sequences them correctly in the datastream.

Figure 2. PPP Multilink Operation



Benefits

MP provides multivendor B-channel aggregation interoperability to the ISDN marketplace. This is especially helpful in the Internet Service Provider marketplace, where many different types of ISDN customer premises equipment (CPE) can be found. MP also addresses some of the issues found with proprietary load-balancing aggregation techniques when using protocols such as IPX or AppleTalk. These protocols are less forgiving of out-of-order packets than IP. By providing sequencing and reordering, MP removes such problems.

Considerations

At present MP is only implemented for dialup circuits. A later release of Cisco IOS software will be enhanced to provide aggregation for any link/interface supporting PPP encapsulation. MP is currently process switched. Due consideration should be given to performance in large hub implementations using multiple ISDN PRIs.

PPP interoperability can never be guaranteed with constantly changing MP software on different vendors' ISDN products. To reduce interoperability problems, Cisco regularly takes part in PPP interoperability testing. MP was last tested at the California ISDN User Group (CIUG) testing session at the Pacific Bell laboratories in mid-September 1995. At that time Cisco successfully interoperated with the following 16 vendors.

Table 4.

Company	Product	Software Release
3Com Corporation	Impact	
3Com Corporation	AccessBuilder 400	6.01 (unreleased)
3Com Corporation	NETBuilder Remote Office	Unreleased software
Ascend	Pipeline Max 4000	4.5
Gandalf	XpressWay	3.2
Eicon Diehl	PacketBlaster	SDK 20
Eicon Technology	SOHO/Connect DIVA	Unreleased software
ISDNtek	Cyberspace Freedom	CY123.2099
Shiva	Shiva PPP Client	4.0
ISC	SecureLink II	Unreleased software
Combinet (now Cisco)	2060	3.1
Microsoft	Windows '95	
Rockwell Network Systems	Dialup Router	4.1
Motorola	Bitsurfer Pro	
Xyplex	Network 3000	5.5
Network Express	Interhub	Unreleased software

IP Address Negotiation for ISDN

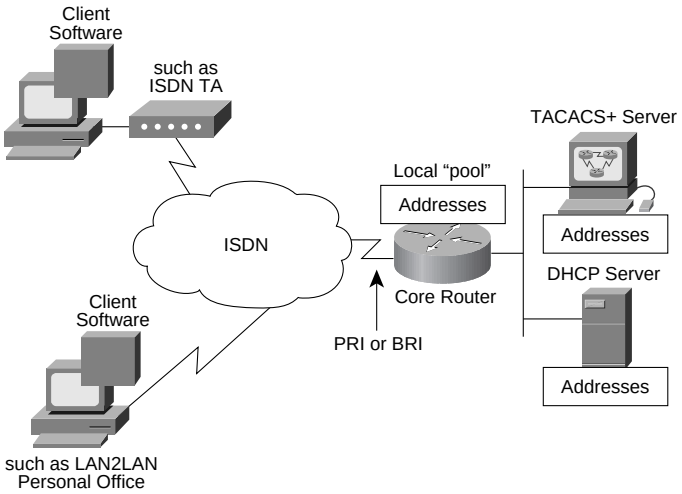
Description

IP Address Negotiation for ISDN allows remote node PPP client software to request an IP address from a Cisco core router during call setup. This request occurs as part of the PPP IPCP setup negotiation.

This feature is specifically designed for remote node connectivity where the end user is operating a PC/Mac/workstation with a nonrouting device such as a Cisco LAN^{2}LAN Personal Office ISDN PC card or an external ISDN terminal adapter such as a Motorola Bitsurfer.

IP addresses can be assigned either from a “local pool” that is held on the core router or from an external TACACS+ or DHCP server. Figure 3 shows the solutions where IP address negotiation can be best utilized.

Figure 3. IP Address Negotiation



Note that multiple pooling types can be active simultaneously on the core router. It is possible for certain dial-up users to be assigned an IP address from a local “pool” while others use a TACACS+ server.

Local Address Pooling

Several pools of IP addresses can be held on the core router. Each pool can hold up to 255 addresses. Each pool has a free queue containing available addresses and a “used” queue containing address currently in use. On receipt of the IPCP address negotiation request, the core router retrieves an address from the free queue. It is possible for the client to request the same address used in his or her last connection. If this address is in the free queue, it will be assigned. If it is in use, another address from the free queue is assigned.

TACACS+ IP Address Assignment

It is possible to configure TACACS+ to assign an IP address to a dial-up user. This can be done in one of two ways. An IP address can be assigned directly by the TACACS+ server while it is authorizing the remote node connection. As an alternative the TACACS+ server can return a local address pool name, which allows the core router to assign the IP address from that local pool.

DHCP

When using DHCP, the core router acts as a DHCP proxy for the remote client. On receipt of the IPCP address negotiation request, the core router retrieves an IP address from the DHCP server. At the end of the session, the router returns that address to the server. For more information on DHCP, see the following World Wide Web URL:

`http://web.syr.edu/~jmwobus/comfaqs/dhcp.faq.html`

Benefits

Address negotiation allows an organization to manage its address space centrally. It also allows the use of IP addresses to be minimized. In most instances, dial-up services are oversubscribed. With address negotiation, it is only necessary to provide enough address space to cope with worst-case loading scenarios. Use of IP address negotiation also reduces configuration text in the core router. Because of the dynamic nature of IP address assignment, it is no longer necessary to maintain a specific dialer map statement for each remote node. IP address negotiation creates dynamic dialer maps for each connection and removes them at the end of the session.

Considerations

It is important to ensure that an address is being negotiated via the PPP IPCP. Some client software stacks such as support DHCP locally. If a DHCP request originates remotely, the core router cannot function as a DHCP proxy, and no return path will be available through this unit.

PPP Callback for ISDN

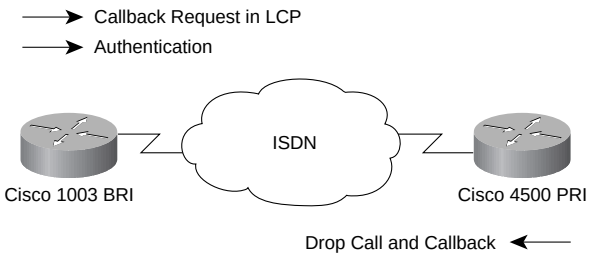
(Refer to the “Cisco 750 Configuration” section for an example of PPP Callback for ISDN on Cisco IOS platforms.)

Description

Callback for ISDN interfaces allows a Cisco router using a DDR interface and PPP encapsulation to initiate a circuit-switched WAN link to another device and request that it be called back. A Cisco ISDN router can also respond to a callback request from a remote device. The process uses PPP and the facilities specified in RFC 1570. A typical negotiation would proceed as follows (see Figure 4):

- Router A brings up a circuit-switched connection to Router B.
- Routers A and B negotiate PPP Link Control Protocol (LCP) with either Router A requesting callback or Router B initiating callback.
- Routers authenticate using PPP PAP or CHAP protocols. Router A is required to authenticate; Router B authentication is optional.
- Circuit-switched connection is dropped by both routers.
- Router B brings up circuit-switched connection to Router A.

Figure 4. PPP Callback Operation



Benefits

Callback for ISDN/DDR provides centralized billing for sync dial-up services. It also allows organizations to take advantage of tariff disparities on both a national and an international basis.

Considerations

Because callback for ISDN/DDR requires a circuit-switched connection to be established before the callback request can be passed, a small charge (dependent on local tariffing) will always be incurred by the router that originally initiates the call.

For more information on these features and the rest of the Cisco IOS ISDN feature set, refer to Cisco Connection Documentation CD-ROM and CCO.

AppleTalk DDR Update

Running AppleTalk over DDR links is problematic because of the number of broadcasts generated by AppleTalk devices. Name Binding Protocol (NBP) packets are at the top of the list of AppleTalk broadcast packets that bring DDR circuits up and down.

A variety of applications including QuarkXpress, FileMaker Pro, and Datebook Pro send out all-zone NBP broadcasts to check for licensing violations. For obvious reasons this is a bad strategy when usage-based DDR links are in use.

To alleviate the effects that NBP traffic imposes on DDR links, Cisco has introduced NBP Filtering with Release 11.0 of the Cisco IOS software.

In Release 11.0 and later, look for the following addition:

```
homer(config) #access-list 601 deny ?
<1-65279>                                AppleTalk network number
additional-zones                         Default filter action for unspecified zones
cable-range                              Filter on cable range
includes                                 Filter on cable range inclusively
nbp                                      Specify nbp filter
network                                  Filter an AppleTalk network
other-access                             Default filter action
other-nbps                               Default filter action for nbp
within                                   Filter on cable range exclusively
zone                                     Filter on AppleTalk zone
```

Under the NBP heading are the following commands:

```
homer(config)#access-list 601 deny nbp ?
   <1-65536> nbp sequence number
homer(config)#access-list 601 deny nbp 1 ?
   object Filter on nbp object
   type Filter on nbp type
   zone Filter on nbp zone
homer(config)#access-list 601 deny nbp 1 object ?
   LINE NBP object filter
homer(config)#access-list 601 deny nbp 1 type ?
   LINE NBP type filter
homer(config)#access-list 601 deny nbp 1 zone ?
   LINE NBP zone filter
```

The following is a sample configuration used to filter all NBPs except AppleShare NBP traffic. All other traffic is permitted using the **other-access** command. Broadcast traffic is not permitted by using the **broadcast-deny** statement.

```
!
access-list 601 permit nbp 1 type AFPServer
access-list 601 deny other-nbps
access-list 601 permit other-access broadcast-deny
!
dialer-list 1 list 601
!
```

To learn more about NBP packets in your LAN/WAN environment, use the NBP Test feature that is available on all Cisco IOS routers. To use this feature, follow the steps below:

cisco-router#

```
cisco-router#ping                              :Invoke the extended ping function

Protocol [ip]: appletalk

Target AppleTalk address: nbp                  :This starts NBPtest facility

nbptest> ?                                     :Type ? for help

Tests are:

lookup: lookup an NVE. prompt for name, type
  and zone

parms: display/change lookup parms (ntimes,
  nsecs, interval)

zones: display zones

poll: for every zone, lookup all devices, using
  default parms

help|?: print command list

quit: exit nbptest


nbptest> parms                                 :Always start by adjusting the parms to these defaults.

maxrequests [5]: 1                              These are TAC recommendations.

maxreplies [1]: 200

interval [5]: 5
```

The example below will lookup all resources in the zone “Infosource”

```
nbptest>

nbptest> lookup

Entity name [=]:                               := is wild card, or type the exact name

Type of Service [=]:                           :i.e., AFPServer

Zone [Twilight]: Infosource                    :Zone of interest

Output deleted due to length
```

The example below looks up the types of services provided by “Sales Server”

```
nbptest> lookup
Entity name [=]: Sales Server
Type of Service [=]:
Zone [Infosource]:
(7214n,35a,244s)[1]<-(7214.35.2)
: ‘Sales Server:AFPServer@Infosource’          :Syntax of output is as follows ‘Entity
(7214n,35a,8s)[1]<-(7214.35.2)                 (object): Type@Zone’
: ‘Sales Server:SNMP Agent@Infosource’        :Syntax of output is as follows ‘Entity
(7214n,35a,4s)[1]<-(7214.35.2)                 (object): Type@Zone’
: ‘Sales Server:Workstation@Infosource’       :Syntax of output is as follows ‘Entity
NBP lookup request timed out                   (object): Type@Zone’
Processed 3 replies, 6 events
nbptest>
nbptest> quit                                 :returns to the router prompt
cisco-router#
```

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
World Wide Web URL:
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Cisco Systems has over 120 sales offices worldwide. To contact your local account representative, call the company's corporate headquarters (California, USA) at 408 526-4000 or in North America call 800 553-NETS (6387).

12/95