Enterprise Dial Scenarios and Configurations

This chapter provides sample configurations for specific dial scenarios used by enterprise networks (not telephone companies or Internet service providers). Each configuration is designed to support IP network traffic with basic security for the specified scenario.

The following scenarios are described:

- Scenario 1—Remote Offices and Telecommuters Dialing In to a Central Site
- Scenario 2—Bidirectional Dial Between Central Sites and Remote Offices
- Scenario 3—Telecommuters Dialing In to a Mixed Protocol Environment

Note If you use Token card-based security in your dial network, we recommend that you enable Password Authentication Protocol (PAP) authentication and disable the Multilink protocol to maximize dial-in performance.

Remote User Demographics

Employees stationed in remote offices or disparate locations often dial in to central sites or headquarter offices to download or upload files and check e-mail. These employees often dial in to the corporate network from a remote office LAN using ISDN or from another location such as a hotel room using a modem.

The following remote enterprise users typically dial in to enterprise networks:

- Full-time telecommuters—Employees using stationary workstations to dial in from a small office, home office (SOHO), making ISDN connections with terminal adapters or PC cards through the public telephone network, and operating at higher speeds over the network, which rules out the need for a modem.
- Travelers—Employees such as salespeople that are not in a steady location for more than 30 percent of the time usually dial in to the network with a laptop and modem through the public telephone network, and primarily access the network to check E-mail or transfer a few files.
- Workday extenders—Employees that primarily work in the company office, occasionally dial in to the enterprise with a mobile or stationary workstation plus modem, and primarily access the network to check E-mail or transfer a few files.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Demand and Scalability

You need to evaluate scalability and design issues before you build a dial enterprise network. As the number of company employees increases, the number of remote users who need to dial in increases. A good dial solution scales upward as the demand for dial-in ports grows. For example, it is not uncommon for a fast-growing enterprise to grow from a demand of 100 modems to 250 modems in less than one year.

You should always maintain a surplus of dial-in ports to accommodate company growth and occasional increases in access demand. In the early stages of a fast-growing company that has 100 modems installed for 6000 registered remote users, only 50 to 60 modems might be active at the same time. As demand grows over one year, 250 modems might be installed to support 10,000 registered token card holders.

During special company occasions, such as worldwide conventions, demand for remote access can also increase significantly. During such activities, dial-in lines are used heavily throughout the day and evening by remote sales people using laptops to access E-mail and share files. This behavior is indicative of sales people working away from their home territories or sales offices. Network administrators need to prepare for these remote access bursts, which cause significant increases for remote access demand.

Remote Offices and Telecommuters Dialing In to a Central Site

Remote office LANs typically dial in to other networks using ISDN. Remote offices that use Frame Relay require a more costly dedicated link.

Connections initiated by remote offices and telecommuters are brought up on an as-needed basis, which results in substantial cost savings for the company. In dial-on-demand scenarios, users are not connected for long periods of time. The number of remote nodes requiring access is relatively low, and the completion time for the dial-in task is short.

Central sites typically do not dial out to the remote LANs. Instead, central sites respond to calls. Remote sites initiate calls. For example, a field sales office might use ISDN to dial in to and browse a central site's intranet. Additionally a warehouse comprising five employees can use ISDN to log in to a remote network server to download or upload product order information. For an example of bidirectional dialing, see the section "Bidirectional Dial Between Central Sites and Remote Offices" later in this chapter.

Note Dial-on-demand routing (DDR) uses static routes or snapshot routing. For IP-only configurations, static routes are commonly used for remote dial-in. For Internet Protocol Exchange (IPX) networking, snapshot routing is often used to minimize configuration complexity.

Network Topologies

Figure 1 shows an example of a remote office that places digital calls in to a central site network. The remote office router can be any Cisco router with a BRI physical interface, such as a Cisco 766 or Cisco 1604 router. The central office gateway router can be any Cisco router that supports PRI connections, such as a Cisco 3600 series, Cisco 4000 series, or Cisco 7000 series router.

Figure 1 Remote Office Dialing In to a Central Site

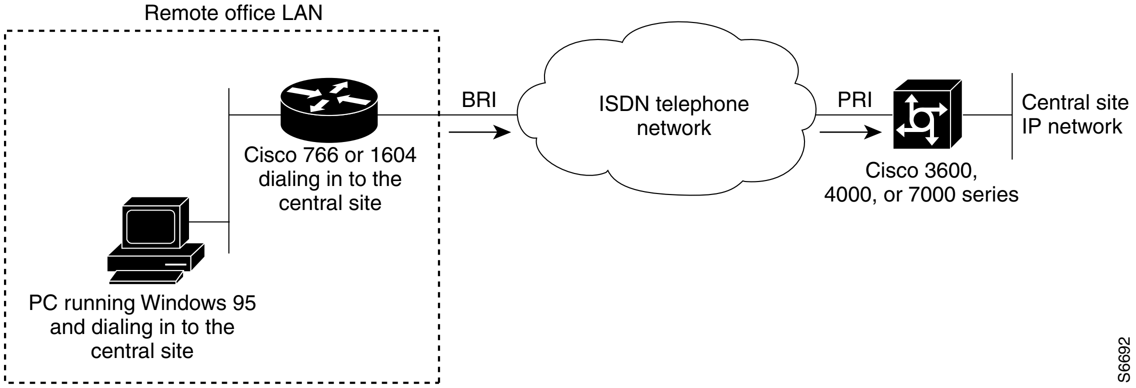
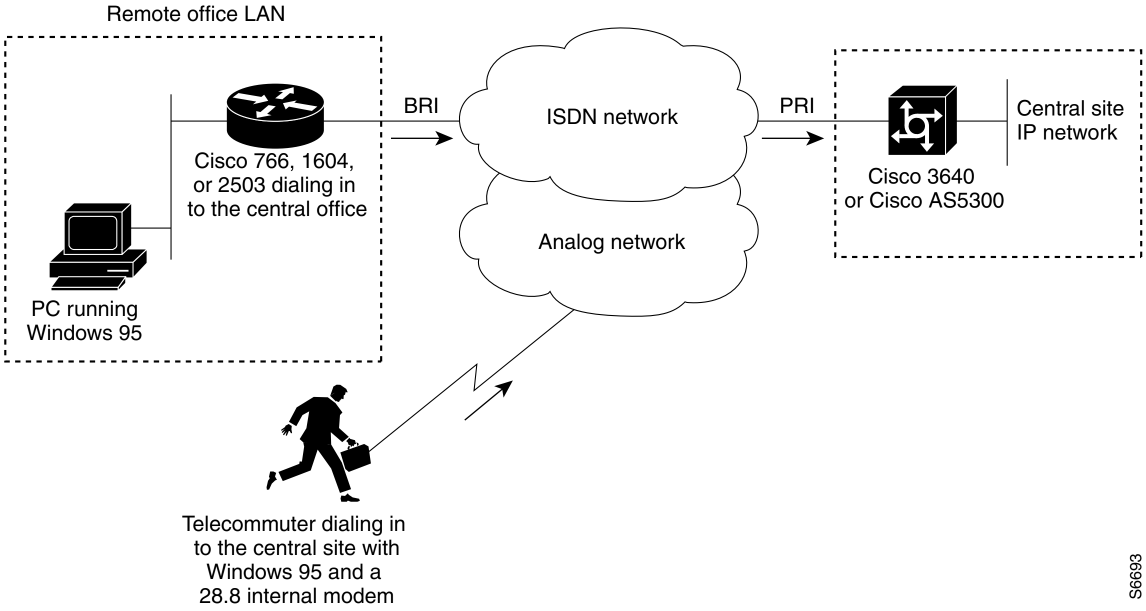

Remote office LAN
Cisco 766 or 1604 dialing in to the central site
PC running Windows 95 and dialing in to the central site
BRI
ISDN telephone network
PRI
Cisco 3600, 4000, or 7000 series
Central site IP network
S6692

Figure 2 shows an example of a remote office and telecommuter dialing in to a central site. The remote office places digital calls. The telecommuter places analog calls. The remote office router can be any Cisco router with a BRI interface, such as a Cisco 766, Cisco 1604, or Cisco 2503 router. The central office gateway router is a Cisco AS5300 series access server or a Cisco 3640 router, which supports both PRI and analog connections.

Figure 2 Remote Office and Telecommuter Dialing In to a Central Site


Remote office LAN
Cisco 766, 1604, or 2503 dialing in to the central office
PC running Windows 95
BRI
ISDN network
Analog network
PRI
Cisco 3640 or Cisco AS5300
Central site IP network
Telecommuter dialing in to the central site with Windows 95 and a 28.8 internal modem
S6693

Dial-In Scenarios

The configuration examples in the following sections provide different combinations of dial-in scenarios, which can be derived from Figure 1 and Figure 2:

- Cisco 1604 Remote Office Router Dialing In to a Cisco 3620 Access Router
- Remote Office Router Dialing In to a Cisco 3620 Router

- Cisco 700 Series Router Using Port Address Translation to Dial In to a Cisco AS5300 Access Server
- Cisco 3640 Central Site Router Configuration to Support ISDN and Modem Calls
- Cisco AS5300 Central Site Configuration Using Remote Security

Note Be sure to include your own IP addresses, host names, and security passwords where appropriate if you use these examples in your own network.

Cisco 1604 Remote Office Router Dialing In to a Cisco 3620 Access Router

This section provides a common configuration for a Cisco 1604 remote office router dialing in to a Cisco 3620 access router positioned at a central enterprise site. Only ISDN digital calls are supported in this scenario. No analog modem calls are supported. All calls are initiated by the remote router on an as-needed basis. The Cisco 3620 router is not set up to dial out to the Cisco 1604 router. (Refer to Figure 1.)

The Cisco 1604 and Cisco 3620 routers use the IP unnumbered address configurations, MLP, and the dial-load threshold feature, which brings up the second B channel when the first B channel exceeds a certain limit. Because static routes are used, a routing protocol is not configured. A default static route is configured on the Cisco 1604 router, which points back to the central site. The central site also has a static route that points back to the remote LAN. Static route configurations assume that you have only one LAN segment at each remote office.

Cisco 1604 Router Configuration

The following configuration runs on the Cisco 1604 router, shown in Figure 1. This SOHO router places digital calls in to the Cisco 3620 central site access router. See the next example for the running configuration of the Cisco 3620 router.

```
version xx.x
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname remotelan1
!
enable secret cisco
!
username NAS password dialpass
username admin password cisco

isdn switch-type basic-5ess
!
interface Ethernet0
 ip address 10.2.1.1 255.255.255.0
!
interface BRI0
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer map ip 10.1.1.10 name NAS 5551234
 dialer load-threshold 100 either
 dialer-group 1
 no fair-queue
 ppp authentication chap pap callin
 ppp multilink
```

```
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.10
ip route 10.1.1.10 255.255.255.255 BRI0
dialer-list 1 protocol ip permit
!
line con 0
line vty 0 4
 login local
!
end
```

Cisco 3620 Router Configuration

The following sample configuration runs on the Cisco 3620 router shown in Figure 1. This modular access router has one 2-port PRI network module installed in slot 1 and one 1-port Ethernet network module installed in slot 0. The router receives only digital ISDN calls from the Cisco 1604 router. The configuration for the Cisco 1604 router was provided in the previous example.

```
version xx.x
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname NAS
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin local
aaa authentication ppp default local
aaa authentication ppp dialin if-needed local
enable secret cisco
!
username admin password cisco
username remotelan1 password dialpass

async-bootp dns-server 10.1.3.1 10.1.3.2
isdn switch-type primary-5ess
!
controller T1 1/0
 framing esf
 clock source line
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1/1
 framing esf
 clock source line
 linecode b8zs
 pri-group timeslots 1-24
!
interface Loopback0
 ip address 10.1.2.254 255.255.255.0
!
interface Ethernet 0/0
 ip address 10.1.1.10 255.255.255.0
 ip summary address eigrp 10 10.1.2.0 255.255.255.0
!
interface Serial 1/0:23
```

```
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Serial 1/1:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Dialer0
 ip unnumbered Loopback0
 no ip mroute-cache
 encapsulation ppp
 peer default ip address pool dialin_pool
 dialer in-band
 dialer-group 1
 no fair-queue
 no cdp enable
 ppp authentication chap pap dialin
 ppp multilink
!
router eigrp 10
 network 10.0.0.0
 passive-interface Dialer0
 default-metric 64 100 250 100 1500
 redistribute static
 no auto-summary
!
ip local pool dialin_pool 10.1.2.1 10.1.2.50
ip default-gateway 10.1.1.1

ip route 10.2.1.1 255.255.255.255 Dialer0
ip route 10.2.1.0 255.255.255.0 10.2.1.1

ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
 login authentication console
line aux 0
 login authentication console
line vty 0 4
 login authentication vty
 transport input telnet rlogin
!
end
```

Remote Office Router Dialing In to a Cisco 3620 Router

This section provides a common configuration for a Cisco 700 or 800 series remote office router placing digital calls in to a Cisco 3620 router positioned at a central enterprise site. All calls are initiated by the remote router on an as-needed basis. The Cisco 3620 router is not set up to dial out to the remote office router. (See Figure 1.)

Cisco 700 Series Router Configuration

The following configuration task is for a Cisco 700 series ISDN router placing digital calls in to a central site router that supports ISDN PRI, such as the Cisco 3620 router. In this scenario, ISDN unnumbered interfaces with static routes are pointing back to the Cisco 3620.

To configure the router, use the following commands in EXEC mode. However, this configuration assumes that you are starting from the router's default configuration. To return the router to its default configuration, issue the **set default** command.

	Command	Purpose

Step 1	`>`
	`> set systemname remotelan1`
	`remotelan1>`
		At the system prompt level, specifies the host name of the router, which is also used when responding to Challenge Handshake Authentication Protocol (CHAP) authentication with the Cisco 3620. For CHAP authentication, the system's name must match the username configured on the Cisco 3620.

Step 2	`remotelan1> set ppp secret client`
	`remotelan1> Enter new password: dialpass`
	`remotelan1> Enter new password: dialpass`
		Sets the transmit and receive password for the client. This is the password which is used in response to CHAP authentication requests, and it must match the username password configured on the Cisco 3620 router.

Step 3	`remotelan1> set encapsulation ppp`	Sets PPP encapsulation for incoming and outgoing authentication instead of CPP.
Step 4	`remotelan1> set ppp multilink on`	Enables Multilink PPP (MLP).

Step 5	`remotelan1> set user nas`
	`remotelan1> New user nas being created`
		Creates the profile named nas, which is reserved for the Cisco 3620 router.

Step 6	`remotelan1:nas> set ip 0.0.0.0`	Specifies the LAN IP address. The sequence 0.0.0.0 means that it will use the address assigned to it from the central Cisco 3620 router. See Step 14.
Step 7	`remotelan1:nas> set ip framing none`	Configures the profiles to not use Ethernet framing.
Step 8	`remotelan1:nas> set ip route destination 0.0.0.0 gateway 10.1.1.10`	Sets the default route to point to the Ethernet IP address of the Cisco 3620 router.
Step 9	`remotelan1:nas> set timeout 300`	Sets the idle time at which the B channel will be dropped. In this case, the line is dropped after 300 seconds of idle time.
Step 10	`remotelan1:nas> set 1/2 number 5551234`	Sets the number to call when dialing out of the first and second B channel.
Step 11	`remotelan1:nas> cd lan`	Enters LAN profile mode.
Step 12	`remotelan1:LAN> set bridging off`	Turns bridging off.
Step 13	`remotelan1:LAN> set ip routing on`	Turns on IP routing.
Step 14	`remotelan1:LAN> set ip address 10.2.1.1`	Sets the LAN IP address for the interface.

After you configure the Cisco 760 or Cisco 770 series router, the final configuration should resemble the following:

```
set systemname remotelan1
set ppp secret client
set encapsulation ppp
set ppp multilink on
cd lan
```

```
set bridging off
set ip routing on
set ip 10.2.1.1
set subnet 255.255.255.0
set user nas
set bridging off
set ip 0.0.0.0
set ip netmask 0.0.0.0
set ip framing none
set ip route destination 0.0.0.0 gateway 10.1.1.10
set timeout 300
set 1 number 5551234
set 2 number 5551234
```

The previous software configuration does not provide for any access security. To provide access security, use the following optional commands in EXEC mode:

Command	Purpose
`Router>` **`set ppp authentication incoming chap`**	Provides CHAP authentication to incoming calls.
`Router>` **`set callerid`**	Requires the calling parties number to be matched against the configured receive numbers (such as set by the **set callidreceive #** command). This command also denies all incoming calls if no callidreceive number is configured.
`Router>` **`set remoteaccess protected`**	Specifies a remote system password, which enables you to make changes on the router from a remote location.
`Router>` **`set localaccess protected`**	Specifies a local system password, which enables you to make changes on the router from a local console connection.
`Router>` **`set password system`**	Sets the system password for the previous access configurations.

Cisco 3620 Router Configuration

The following example provides a sample configuration for the Cisco 3620 router. This modular access router has one 2-port PRI network module installed in slot 1 and one 1-port Ethernet network module installed in slot 0. The router receives only digital ISDN calls over T1 lines from the Cisco 700 series remote office router, which was described in the previous example.

```
version xx.x
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
hostname NAS
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin local
aaa authentication ppp default local
aaa authentication ppp dialin if-needed local
enable secret cisco
!
username admin password cisco
username remotelan1 password dialpass
!
async-bootp dns-server 10.1.3.1 10.1.3.2
isdn switch-type primary-5ess
!
controller T1 1/0
 framing esf
 clock source line
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1/1
 framing esf
 clock source line
 linecode b8zs
 pri-group timeslots 1-24
!
interface Loopback0
 ip address 10.1.2.254 255.255.255.0
!
interface Ethernet 0/0
 ip address 10.1.1.10 255.255.255.0
 ip summary address eigrp 10 10.1.2.0 255.255.255.0
!
interface Serial 1/0:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Serial 1/1:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Dialer0
 ip unnumbered Loopback0
 no ip mroute-cache
 encapsulation ppp
 peer default ip address pool dialin_pool
 dialer in-band
 dialer-group 1
 no fair-queue
 no cdp enable
 ppp authentication chap pap dialin
 ppp multilink
!
router eigrp 10
 network 10.0.0.0
 passive-interface Dialer0
 default-metric 64 100 250 100 1500
 redistribute static
 no auto-summary
!
ip local pool dialin_pool 10.1.2.1 10.1.2.50
ip default-gateway 10.1.1.1
ip route 10.2.1.1 255.255.255.255 Dialer0
ip route 10.2.1.0 255.255.255.0 10.2.1.1

ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
 login authentication console
line aux 0
 login authentication console
line vty 0 4
 login authentication vty
 transport input telnet rlogin
!
end
```

Cisco 700 Series Router Using Port Address Translation to Dial In to a Cisco AS5300 Access Server

This section shows a Cisco 700 series router using the port address translation (PAT) feature to dial in to a Cisco AS5300 central site access server. IP addresses are assigned from the central site, which leverages the PAT feature to streamline multiple devices at the remote site through a single assigned address. In this example, the Cisco 700 series router has a private range of IP addresses used on the Ethernet side. However, the router is able to translate between the local private addresses and the dynamically registered address on the WAN interface. (See Figure 1.)

Cisco 700 Series Configuration

The sample configuration in this section allows PCs on a LAN to boot up and acquire their IP address dynamically from a Cisco 700 series router, which in turn translates the private addresses into a single IP address assigned from a Cisco AS5300 central site router. The Cisco 700 series router also passes information via DHCP regarding the Domain Name System (DNS) server (in this example, 10.2.10.1) and the Windows Internet naming service (WINS) server (in this example, 10.2.11.1) along with the domain name.

A possible sequence of events would be a remote PC running Windows 95 boots up on the Ethernet segment and gets its IP address and network information from the Cisco 700 series router. The PC then opens up Netscape and attempts to view a web page at the central site, which causes the router to dial in to the central site. The router dynamically obtains its address from the central site pool of addresses and uses it to translate between the private address on the local Ethernet segment and the registered IP address borrowed from the central site router.

To configure a remote router, use the following commands beginning in EXEC mode:

	Command	Purpose

Step 1	`>`
	`>` **`set systemname remotelan1`**
	`Router>`
		At the system prompt level, specifies the host name of the router, which is also used when responding to CHAP authentication with the Cisco 3620 router. For CHAP authentication, the system's name must match the username configured on the Cisco 3620.

Step 2	`Router>` **`set ppp secret client`**
	`Router> Enter new password:` **`dialpass`**
	`Router> Enter new password:` **`dialpass`**
		Sets the transmit and receive password for the client. This is the password which is used in response to CHAP authentication requests, and it must match the username password configured on the Cisco 3620 router.

	Command	Purpose
Step 3	`Router> set encapsulation ppp`	Sets PPP encapsulation for incoming and outgoing authentication instead of CPP.
Step 4	`Router> set ppp multilink on`	Enables MLP.
Step 5	`Router> set dhcp server`	Enables the router to act as a DHCP server and assign addresses from the private network. By default, all DHCP client addresses are assigned from the 10.0.0.0 network.
Step 6	`Router> set dhcp dns primary 10.2.10.1`	Passes the DNS server IP address to the DHCP client.
Step 7	`Router> set dhcp wins 10.2.11.1`	Passes the IP address of the WINS server to the DHCP client.
Step 8	`Router> set dhcp domain nas.com`	Sets the DHCP domain name for the Cisco 3620 central site router.

Step 9	`Router> set user nas`
	`Router> New user nas being created`
		Creates the profile named nas, which is setup for the Cisco 3620 router.

Step 10	`Router:nas> set ip pat on`	Enables Port Address Translation (PAT) on the router.
Step 11	`Router:nas> set ip framing none`	Configures the profiles to not use Ethernet framing.
Step 12	`Router:nas> set ip route destination 0.0.0.0 gateway 10.1.1.0`	Sets the default route to point to the Ethernet IP address of Cisco 3620 router.
Step 13	`Router:nas> set 1 number 5551234`	Sets the number to call when dialing out of the first B channel.
Step 14	`Router:nas> set 2 number 5551234`	Sets the number to call when dialing out of the second B channel.
Step 15	`Router:nas> cd lan`	Enters LAN profile mode.
Step 16	`Router:LAN> set bridging off`	Turns bridging off.
Step 17	`Router:LAN> set ip routing on`	Turns IP routing on.

After you configure the router, the configuration should resemble the following:

```
set systemname remotelan1
set encapsulation ppp
set ppp secret client
set ppp multilink on
set dhcp server
set dhcp dns primary 10.2.10.1
set dhcp wins 10.2.11.1
set dhcp domain nas.com
set user nas
set bridging off
set ip routing on
set ip framing none
set ip pat on
set ip route destination 0.0.0.0 gateway 10.1.1.0
set 1 number 5551234
set 2 number 5551234
```

Cisco AS5300 Router Configuration

The following example configures a Cisco AS5300 router for receiving calls from the router in the previous example.

Note This configuration can also run on a Cisco 4000, Cisco 3600, or Cisco 7000 series router. However, the interface numbering scheme for these routers will be in the form of slot/port. Additionally, the clocking will be set differently. Refer to your product configuration guides and configuration notes for more details.

```
!
version xx.x
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname NAS
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin local
aaa authentication ppp default local
aaa authentication ppp dialin if-needed local
enable secret cisco
!
username admin password cisco
username remotelan1 password dialpass
!
async-bootp dns-server 10.1.3.1 10.1.3.2
isdn switch-type primary-5ess
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Loopback0
 ip address 10.1.2.254 255.255.255.0
!
interface Ethernet0
 ip address 10.1.1.10 255.255.255.0
 ip summary address eigrp 10 10.1.2.0 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface Serial0:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Serial1:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Dialer0
 ip unnumbered Loopback0
 no ip mroute-cache
 encapsulation ppp
 peer default ip address pool dialin_pool
 dialer in-band
 dialer-group 1
 no fair-queue
 no cdp enable
 ppp authentication chap pap dialin
 ppp multilink
!
router eigrp 10
 network 10.0.0.0
 passive-interface Dialer0
 default-metric 64 100 250 100 1500
 redistribute static
 no auto-summary
!
ip local pool dialin_pool 10.1.2.1 10.1.2.50
ip default-gateway 10.1.1.1

ip route 10.2.1.1 255.255.255.255 Dialer0
ip route 10.2.1.0 255.255.255.0 10.2.1.1

ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
 login authentication console
line aux 0
 login authentication console
line vty 0 4
 login authentication vty
 transport input telnet rlogin
!
end
```

In this configuration, the local pool is using a range of unused addresses on the same subnet on which the Ethernet interface is configured. The addresses will be used for the remote devices dialing in to the Cisco AS5300 access server.

Cisco 3640 Central Site Router Configuration to Support ISDN and Modem Calls

The following configuration allows remote LANs and standalone remote users with modems to dial in to a central site. Figure 2 shows the network topology.

The Cisco 3640 router has the following hardware configuration for this scenario:

- One 2-port ISDN-PRI network module installed in slot 1.
- One digital modem network module installed in slot 2 and slot 3.
- One 1-port Ethernet network module installed in slot 0.

Note Each MICA technologies digital modem card has its own group async configuration. Additionally, a single range of asynchronous lines is used for each modem card. For additional interface numbering information, refer to the document *Digital Modem Network Module Configuration Note*.

```
version xx.x
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname NAS
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin local
aaa authentication ppp default local
aaa authentication ppp dialin if-needed local
enable secret cisco
!
username admin password cisco
username remotelan1 password dialpass1
username remotelan2 password dialpass2
username PCuser1 password dialpass3
username PCuser2 password dialpass4
!
async-bootp dns-server 10.1.3.1 10.1.3.2
isdn switch-type primary-5ess
!
controller T1 1/0
 framing esf
 clock source line
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1/1
 framing esf
 clock source line
 linecode b8zs
 pri-group timeslots 1-24
!
interface Loopback0
 ip address 10.1.2.254 255.255.255.0
!
interface Ethernet0/0
 ip address 10.1.1.10 255.255.255.0
 ip summary address eigrp 10 10.1.2.0 255.255.255.0
!
interface Serial 1/0:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Serial 1/1:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Group-Async1
 ip unnumbered Loopback0
 encapsulation ppp
 async mode interactive
 peer default ip address pool dialin_pool
 no cdp enable
 ppp authentication chap pap dialin
 group-range 65 88
!
interface Group-Async2
 ip unnumbered Loopback0
 encapsulation ppp
 async mode interactive
 peer default ip address pool dialin_pool
 no cdp enable
 ppp authentication chap pap dialin
 group-range 97 120
!
interface Dialer0
 ip unnumbered Loopback0
 no ip mroute-cache
 encapsulation ppp
 peer default ip address pool dialin_pool
 dialer in-band
 dialer-group 1
 no fair-queue
 no cdp enable
 ppp authentication chap pap dialin
 ppp multilink
!
router eigrp 10
 network 10.0.0.0
 passive-interface Dialer0
 no auto-summary
!
ip local pool dialin_pool 10.1.2.1 10.1.2.50
ip default-gateway 10.1.1.1
ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
 login authentication console
line 65 88
 autoselect ppp
 autoselect during-login
 login authentication dialin
 modem DialIn
line 97 120
 autoselect ppp
 autoselect during-login
 login authentication dialin
 modem DialIn
line aux 0
 login authentication console
line vty 0 4
 login authentication vty
 transport input telnet rlogin
!
end
```

Cisco AS5300 Central Site Configuration Using Remote Security

The previous examples in this section configured static CHAP authentication on the central router using the **username** command. A more common configuration to support modem and ISDN calls on a single chassis is to use the AAA security model and an external security server at the central site. We recommend that you have a solid understanding of basic security principles and the AAA model before you set up this configuration. For more information about security, see the *Cisco IOS Security Configuration Guide*.

Central Site Cisco AS5300 Configuration Using TACACS+ Authentication

The following example assumes that you are running TACACS+ on the remote security server:

```
version xx.x
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname NAS
!
aaa new-model
aaa authentication login console enable
aaa authentication login vty tacacs+
aaa authentication login dialin tacacs+
aaa authentication ppp default tacacs+
aaa authentication ppp dialin if-needed tacacs+
enable secret cisco
!
async-bootp dns-server 10.1.3.1 10.1.3.2
isdn switch-type primary-5ess
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Loopback0
 ip address 10.1.2.254 255.255.255.0
!
interface Ethernet0
 ip address 10.1.1.10 255.255.255.0
 ip summary address eigrp 10 10.1.2.0 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface Serial0:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Serial1:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Group-Async1
 ip unnumbered Loopback0
 encapsulation ppp
 async mode interactive
 peer default ip address pool dialin_pool
 no cdp enable
 ppp authentication chap pap dialin
 group-range 1 48
!
interface Dialer0
 ip unnumbered Loopback0
 no ip mroute-cache
 encapsulation ppp
 peer default ip address pool dialin_pool
 dialer in-band
 dialer-group 1
 no fair-queue
 no cdp enable
 ppp authentication chap pap dialin
 ppp multilink
!
router eigrp 10
 network 10.0.0.0
 passive-interface Dialer0
 redistribute static
 default-metric 64 100 250 100 1500
 no auto-summary
!
ip local pool dialin_pool 10.1.2.1 10.1.2.50
ip default-gateway 10.1.1.1
ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
 login authentication console
```

```
line 1 48
 autoselect ppp
 autoselect during-login
 login authentication dialin
 modem DialIn
line aux 0
 login authentication console
line vty 0 4
 login authentication vty
 transport input telnet rlogin
end
```

TACACS+ Security Server Entry

The following example can be configured on a remote TACACS+ security server, which complements the Cisco AS5300 access server configuration listed in the previous example:

```
user = remotelan1 {
           chap = cleartext "dialpass1"
           service = ppp protocol = ip {
                       addr = 10.2.1.1
                       route = "10.2.1.0 255.255.255.0"
           }
}


user = PCuser1 {
           login = cleartext "dialpass2"
           chap = cleartext "dialpass2"
           service = ppp protocol = ip {
                       addr-pool = dialin_pool
           }
           service = exec {
                       autocmd = "ppp negotiate"
           }
}

user = PCuser2 {
           login = cleartext "dialpass3"
           chap = cleartext "dialpass3"
           service = ppp protocol = ip {
                       addr-pool = dialin_pool
           }
           service = exec {
                       autocmd = "ppp negotiate"
           }
```

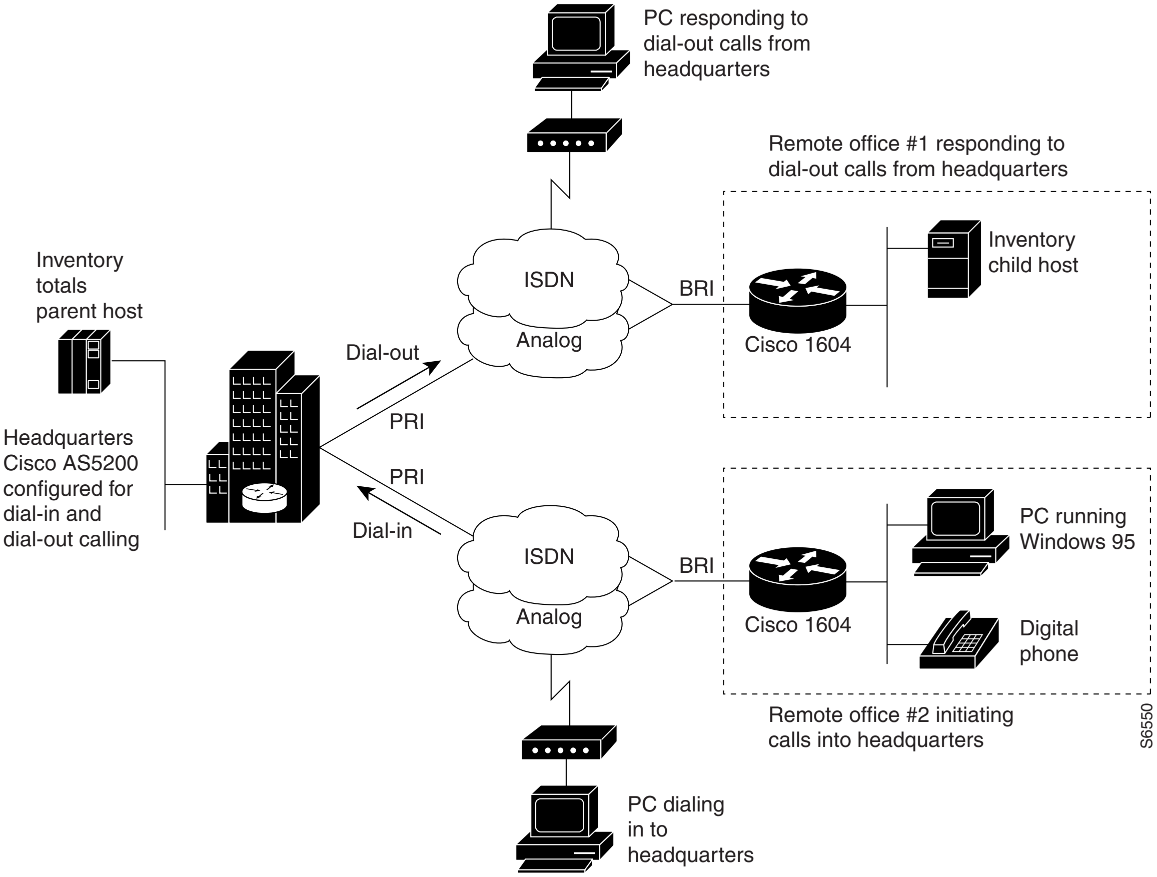
Bidirectional Dial Between Central Sites and Remote Offices

Sometimes a gateway access server at headquarters is required to dial out to a remote site while simultaneously receiving incoming calls. This type of network is designed around a specific business support model.

Dial-In and Dial-Out Network Topology

Figure 3 shows a typical dial-in and dial-out network scenario, which amounts to only 25 percent of all dial topologies. The Cisco AS5300 access server at headquarters initiates a connection with a Cisco 1604 router at remote office 1. After a connection is established, the file server at the remote site (shown as Inventory child host) runs a batch processing application with the mainframe at headquarters (shown as Inventory totals parent host). While files are being transferred between remote office 1 and headquarters, remote office 2 is successfully dialing in to headquarters.

Figure 3 Headquarters Configured for Dial-In and Dial-out Networking


PC responding to dial-out calls from headquarters
Remote office #1 responding to dial-out calls from headquarters
Inventory child host
Inventory totals parent host
ISDN
Analog
BRI
Cisco 1604
Dial-out
PRI
Headquarters Cisco AS5200 configured for dial-in and dial-out calling
PRI
Dial-in
PC running Windows 95
ISDN
Analog
BRI
Cisco 1604
Digital phone
Remote office #2 initiating calls into headquarters
S6550
PC dialing in to headquarters

There are some restrictions for dial-out calling. Dial-out analog and digital calls are commonly made to remote ISDN routers, such as the Cisco 1604 router. On the whole, dial out calls are not made from a central site router to a remote PC but rather from a remote PC in to the central site. However, central site post offices often call remote office routers on demand to deliver E-mail. Callback is enabled on dial-in scenarios only. The majority of a dial out software configuration is setup on the router at headquarters, not the remote office router. Dialing out to a stack group of multiple chassis is not supported by Cisco IOS software. Note that Multichassis Multilink PPP (MMP) and virtual private dialup networks (VPDNs) are dial-in only solutions.

Dialer Profiles and Virtual Profiles

Profiles are set up to discriminate access on a user-specific basis. For example, if the chief network administrator is dialing in to the enterprise, a unique user profile can be created with an idle timeout of one year, and universal access privileges to all networks in the company. For less fortunate users, access can be restricted to an idle timeout of 10 seconds and network connections setup for only a few addresses.

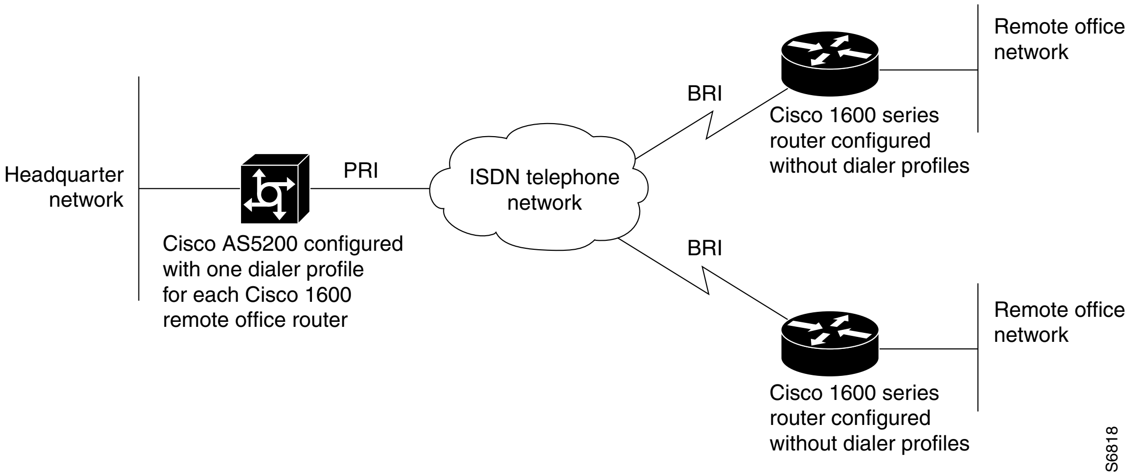
Depending on the size and scope of your dial solution, you can set up two different types of profiles: dialer profiles or virtual profiles. Dialer profiles are individual user profiles set up on routers or access servers in a small-scale dial solution. This type of profile is configured locally on the router and is limited by the number of interfaces that exist on the router. When an incoming call comes into the dial pool, the dialer interface binds the caller to a dialer profile via the caller ID or the caller name.

Figure 4 shows an example of how dialer profiles can be used when:

- You need to bridge over multiple ISDN channels.
- You want to use ISDN to back up a WAN link, but still have the ISDN interface available during those times that the WAN link is up.
- A security server, such as a AAA TACACS or RADIUS server, is not available for use.

Note For more information about dialer profiles, see the chapters "Configuring Peer-to-Peer DDR with Dialer Profiles" and "Configuring Dial Backup with Dialer Profiles."

Figure 4 Dial-In Scenario for Dialer Profiles


Headquarter network
PRI
Cisco AS5200 configured with one dialer profile for each Cisco 1600 remote office router
ISDN telephone network
BRI
BRI
Remote office network
Cisco 1600 series router configured without dialer profiles
Remote office network
Cisco 1600 series router configured without dialer profiles
S6818

Virtual profiles are user-specific profiles for large-scale dial solutions; however, these profiles are not manually configured on each router or access server. A virtual profile is a unique PPP application that can create and configure a virtual access interface dynamically when a dial-in call is received, and tear down the interface dynamically when the call ends.

The configuration information for a virtual access interface in a virtual profile can come from the virtual template interface, or from user-specific configuration information stored on an AAA server, or both. The virtual profile user-specific configuration stored on the AAA server is identified by the authentication name for the call-in user. (That is, if the AAA server authenticates the user as samson, the user-specific configuration is listed under samson in the AAA user file.) The virtual profile user-specific configuration should include only the configuration that is not shared by multiple users. Shared configuration should be placed in the virtual template interface, where it can be cloned on many virtual access interfaces as needed.

AAA configurations are much easier to manage for large numbers of dial-in users. Virtual profiles can span across a group of access servers, but a AAA server is required. Virtual profiles are set up independently of which access server, interface, or port number users connect to. For users that share duplicate configuration information, it is best to enclose the configuration in a virtual template. This requirement eliminates the duplication of commands in each of the user records on the AAA server.

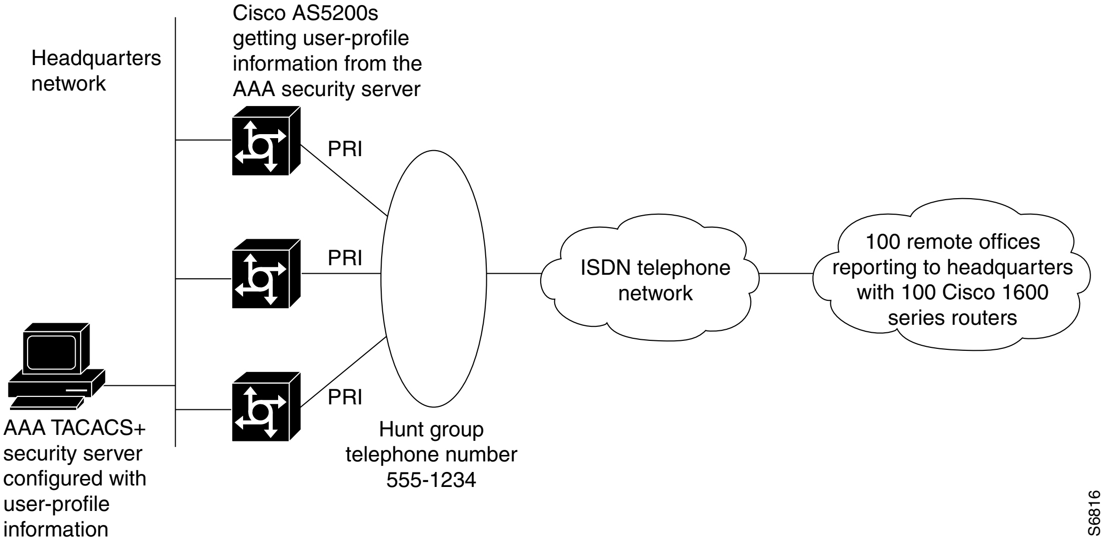
The user-specific AAA configuration used by virtual profiles is interface configuration information and downloaded during link control protocol (LCP) negotiations. Another feature, called per-user configuration, also uses configuration information gained from a AAA server. However, per-user configuration uses *network* configuration (such as access lists and route filters) downloaded during NCP negotiations.

Figure 5 shows an example of how virtual profiles are used:

- A large-scale dial-in solution is available, which includes many access servers or routers (for example, three or more devices stacked together in an MMP scenario).
- Discrimination between large numbers of users is needed.
- Setup and maintenance of a user profile for each dial-in user on each access server or router is much too time consuming.
- A security server, such as a AAA TACACS or RADIUS server, is available for use.

Note For a virtual profile configuration example, see the section "Large-Scale Dial-In Configuration Using Virtual Profiles" later in this chapter. For more information about virtual profiles, see the chapters "Configuring Virtual Profiles" and "Configuring Per-User Configuration" in this publication.

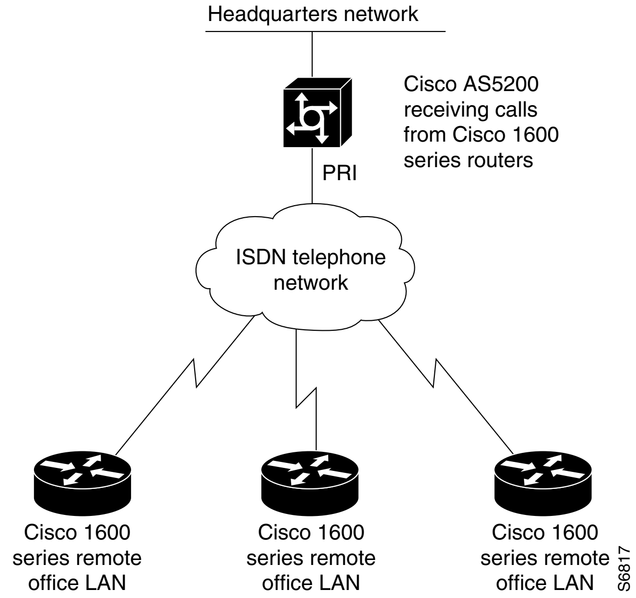
Figure 5 Dial-In Scenario for Virtual Profiles


Headquarters network
Cisco AS5200s getting user-profile information from the AAA security server
PRI
PRI
PRI
ISDN telephone network
100 remote offices reporting to headquarters with 100 Cisco 1600 series routers
AAA TACACS+ security server configured with user-profile information
Hunt group telephone number 555-1234
S6816

Running Access Server Configurations

In most cases, dialer profiles are configured on access servers or routers that receive calls and must discriminate between users, such as many different remote routers dialing in. (See Figure 6.)

Figure 6 Remote Cisco 1600s Dialing In to a Cisco AS5300 at the Central Site



Access servers or routers that only place calls (not receive calls) do not need any awareness of configured dialer profiles. Remote routers do not need to discriminate on the basis of which device they are calling in to. For example, if multiple Cisco 1600 series routers are dialing in to one Cisco AS5300 access server, the Cisco 1600 series routers should not be configured with dialer profiles. The Cisco AS5300 access server should be configured with dialer profiles. Do not configure dialer profiles on devices that *only* make calls.

The configurations examples in the following section are provided for different types of dial scenarios, which can be derived from Figure 3 through Figure 6:

- Examples with dialer profiles:
  - Cisco AS5300 Access Server Configuration with Dialer Profiles
  - Cisco 1604 ISDN Router Configuration with Dialer Profiles
  - Cisco 1604 Router Asynchronous Configuration with Dialer Profiles
- Examples without dialer profiles:
  - Cisco AS5300 Access Server Configuration Without Dialer Profiles
  - Cisco 1604 ISDN Router Configuration Without Dialer Profiles
  - Cisco 1604 Router Asynchronous Configuration Without Dialer Profiles
- Large-Scale Dial-In Configuration Using Virtual Profiles

Note Be sure to include your own IP addresses, host names, and security passwords where appropriate if configuring these examples in your network.

Cisco AS5300 Access Server Configuration with Dialer Profiles

The following bidirectional dial configuration runs on the Cisco AS5300 access server at headquarters in Figure 3. This configuration enables calls to be sent to the SOHO router and received from remote hosts and clients. The calling is bidirectional.

```
version xx.x
service udp-small-servers
service tcp-small-servers
!
hostname 5300
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin local
aaa authentication ppp default local
aaa authentication ppp dialin if-needed local
enable secret cisco
!
username async1 password cisco
username async2 password cisco
username async3 password cisco
username async4 password cisco
username async5 password cisco
username async6 password cisco
username async7 password cisco
username async8 password cisco
username isdn1 password cisco
username isdn2 password cisco
username isdn3 password cisco
username isdn4 password cisco
username isdn5 password cisco
username isdn6 password cisco
username isdn7 password cisco
username isdn8 password cisco
username DialupAdmin password cisco
!
isdn switch-type primary-dms100
chat-script cisco-default ABORT ERROR "" "AT" OK "ATDT\T" TIMEOUT 60 CONNECT
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary
 linecode b8zs
 pri-group timeslots 1-24
!
interface loopback 1
 ip address 172.18.38.40 255.255.255.128
!
interface loopback 2
 ip address 172.18.38.130 255.255.255.128
!
interface Ethernet0
 ip address 172.18.39.40 255.255.255.0
 no ip mroute-cache
 ip ospf priority 0
!
interface Serial0:23
 no ip address
 no ip mroute-cache
 encapsulation ppp
 isdn incoming-voice modem
 dialer pool-member 2
!
interface Serial1:23
 no ip address
 no ip mroute-cache
 encapsulation ppp
 isdn incoming-voice modem
 dialer pool-member 2
!
interface Group-Async1
 no ip address
 no ip mroute-cache
 encapsulation ppp
 async mode interactive
 dialer in-band
 dialer pool-member 1
 ppp authentication chap pap
 group-range 1 48
!
interface Dialer10
 ip unnumbered loopback 1
 encapsulation ppp
 peer default ip address dialin_pool
 dialer remote-name async1
 dialer string 14085268983
 dialer hold-queue 10
 dialer pool 1
 dialer-group 1
 ppp authentication pap chap callin
 ppp pap sent-username DialupAdmin password 7 07063D11542
!
interface Dialer11
 ip unnumbered loopback 1
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name async2
 dialer string 14085262012
 dialer hold-queue 10
 dialer pool 1
 dialer-group 1
 ppp authentication pap chap callin
 ppp pap sent-username DialupAdmin password 7 07063D11542
!
interface Dialer12
 ip unnumbered loopback 1
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name async3
 dialer string 14085260706
 dialer hold-queue 10
 dialer pool 1
 dialer-group 1
 ppp authentication pap chap callin
 ppp pap sent-username DialupAdmin password 7 07063D11542
!
interface Dialer13
 ip unnumbered loopback 1
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name async4
 dialer string 14085262731
 dialer hold-queue 10
 dialer pool 1
 dialer-group 1
 ppp authentication pap chap callin
 ppp pap sent-username DialupAdmin password 7 07063D11542
!
interface Dialer14
 ip unnumbered loopback 1
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name async5
 dialer string 14085264431
 dialer hold-queue 10
 dialer pool 1
 dialer-group 1
 ppp authentication pap chap callin
 ppp pap sent-username DialupAdmin password 7 07063D11542
!
interface Dialer15
 ip unnumbered loopback 1
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name async6
 dialer string 14085261933
 dialer hold-queue 10
 dialer pool 1
 dialer-group 1
 ppp authentication pap chap callin
 ppp pap sent-username DialupAdmin password 7 07063D11542
!
interface Dialer16
 ip unnumbered loopback 1
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name async7
 dialer string 14085267631
 dialer hold-queue 10
 dialer pool 1
 dialer-group 1
 ppp authentication pap chap callin
 ppp pap sent-username DialupAdmin password 7 07063D11542
!
interface Dialer17
 ip unnumbered loopback 2
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name async8
 dialer string 14085265153
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
interface Dialer18
 ip unnumbered loopback 2
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name isdn1
 dialer string 14085267887
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
interface Dialer19
 ip unnumbered loopback 2
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name isdn2
 dialer string 14085261591
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
interface Dialer20
 ip unnumbered loopback 2
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name isdn3
 dialer string 14085262118
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
interface Dialer21
 ip unnumbered loopback 2
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name isdn4
 dialer string 14085263757
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
interface Dialer22
 ip unnumbered loopback 2
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name isdn5
 dialer string 14085263769
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
interface Dialer23
 ip unnumbered loopback 2
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name isdn6
 dialer string 14085267884
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
interface Dialer24
 ip unnumbered loopback 2
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name isdn7
 dialer string 14085267360
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
interface Dialer25
 ip unnumbered loopback 2
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name isdn8
 dialer string 14085260361
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
router ospf 1
redistribute static subnets
passive-interface Dialer1
passive-interface Dialer2
network 172.18.0.0 0.0.255.255 area 0
!
ip local pool dialin_pool 10.1.2.1 10.1.2.50
ip domain-name cisco.com
ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line 1 24
 no exec
 exec-timeout 0 0
 autoselect during-login
 autoselect ppp
 script dialer cisco-default
 login local
 modem InOut
 modem autoconfigure type microcom_hdms
 transport input telnet
line aux 0
line vty 0 1
 exec-timeout 60 0
 password cisco
 login
line vty 2 5
 exec-timeout 5 0
 password cisco
 login
!
end
```

Cisco 1604 ISDN Router Configuration with Dialer Profiles

The following configuration runs on the remote office Cisco 1604 router, which receives calls from the Cisco AS5300 central site access server. (See Figure 3.)

```
version xx.x
service udp-small-servers
service tcp-small-servers
!
```

```
hostname isdn1
!
enable password cisco
!
username 5300 password cisco
username isdn1 password cisco
isdn switch-type basic-5ess
!
interface Ethernet0
 ip address 172.18.40.1 255.255.255.0
!
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 1
 ppp authentication chap pap
!
interface Dialer1
 ip address 172.18.38.131 255.255.255.128
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name 5300
 dialer string 14085269328
 dialer hold-queue 10
 dialer pool 2
 dialer-group 1
 ppp authentication chap pap
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.38.130
dialer-list 1 protocol ip permit
!
line con 0
line vty 0 4
 password cisco
 login
 password cisco
 login
!
end
```

Cisco 1604 Router Asynchronous Configuration with Dialer Profiles

The following asynchronous configuration runs on the remote office Cisco 1604 router, which receives calls from the Cisco AS5300 central site access server. (See Figure 3.)

```
version xx.x
service udp-small-servers
service tcp-small-servers
!
hostname async1
!
enable password cisco
!
username 5300 password cisco
username async1 password cisco
chat script dial_out "" "ATDT\T" timeout 60 connect \c
!
interface Ethernet0
 ip address 172.18.41.1 255.255.255.0
!
interface serial 0
```

```
 physical-layer async
 no ip address
 encapsulation ppp
 dialer pool-member 1
 ppp authentication chap pap
!
interface Dialer10
 ip address 172.18.38.41 255.255.255.128
 encapsulation ppp
 no peer default ip address pool
 dialer remote-name 5300
 dialer string 14085269328
 dialer hold-queue 10
 dialer pool 1
 dialer-group 1
 ppp authentication chap pap
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.38.40
dialer-list 1 protocol ip permit
!
line con 0
line 1
password cisco
login
script modem dial_out
!
end
```

Cisco AS5300 Access Server Configuration Without Dialer Profiles

The following bidirectional dial configuration runs on the Cisco AS5300 access server at headquarters in Figure 3. This configuration enables calls to be sent to the SOHO router and received from remote hosts and clients. The calling is bidirectional.

```
version xx.x
service udp-small-servers
service tcp-small-servers
!
hostname 5300
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin local
aaa authentication ppp default local
aaa authentication ppp dialin if-needed local
enable secret cisco
!
username async1 password cisco
username async2 password cisco
username async3 password cisco
username async4 password cisco
username async5 password cisco
username async6 password cisco
username async7 password cisco
username async8 password cisco
username isdn1 password cisco
username isdn2 password cisco
username isdn3 password cisco
username isdn4 password cisco
username isdn5 password cisco
username isdn6 password cisco
username isdn7 password cisco
username isdn8 password cisco
username DialupAdmin password cisco
!
isdn switch-type primary-dms100
chat-script cisco-default ABORT ERROR "" "AT" OK "ATDT\T" TIMEOUT 60 CONNECT
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
 description ISDN Controller 0
!
controller T1 1
 framing esf
 clock source line secondary
 linecode b8zs
 pri-group timeslots 1-24
 description ISDN Controller 1
!
interface Ethernet0
 ip address 172.18.39.40 255.255.255.0
 no ip mroute-cache
 ip ospf priority 0
!
interface Serial0:23
 no ip address
 no ip mroute-cache
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 2
!
interface Serial1:23
 no ip address
 no ip mroute-cache
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 2
!
interface Group-Async1
 no ip address
 no ip mroute-cache
 encapsulation ppp
 async dynamic address
 async mode interactive
 dialer in-band
 dialer rotary-group 1
 ppp authentication pap callin
 ppp pap sent-username HQ5300 password 7 09434678520A
 group-range 1 24
!
interface Dialer1
 ip address 172.18.38.40 255.255.255.128
 encapsulation ppp
 no peer default ip address pool
 dialer in-band
 dialer map ip 172.18.38.41 name async1 14445558983
 dialer map ip 172.18.38.42 name async2 14445552012
 dialer map ip 172.18.38.43 name async3 14445550706
 dialer map ip 172.18.38.44 name async4 14445552731
 dialer map ip 172.18.38.45 name async5 14445554431
 dialer map ip 172.18.38.46 name async6 14445551933
 dialer map ip 172.18.38.47 name async7 14445557631
 dialer map ip 172.18.38.48 name async8 14445555153
 dialer hold-queue 10
 dialer-group 1
 ppp authentication pap chap callin
 ppp pap sent-username DialupAdmin password 7 07063D11542
!
interface Dialer2
 ip address 172.18.38.130 255.255.255.128
 encapsulation ppp
 no peer default ip address pool
 dialer in-band
 dialer map ip 172.18.38.131 name isdn1 14445557887
 dialer map ip 172.18.38.132 name isdn2 14445551591
 dialer map ip 172.18.38.133 name isdn3 14445552118
 dialer map ip 172.18.38.134 name isdn4 14445553757
 dialer map ip 172.18.38.135 name isdn5 14445553769
 dialer map ip 172.18.38.136 name isdn6 14445557884
 dialer map ip 172.18.38.137 name isdn7 14445557360
 dialer map ip 172.18.38.138 name isdn8 14445550361
 dialer hold-queue 10
 dialer-group 1
 ppp authentication chap pap
 ppp multilink
!
router ospf 1
 redistribute static subnets
 passive-interface Dialer1
 passive-interface Dialer2
 network 172.18.0.0 0.0.255.255 area 0
!
ip domain-name cisco.com
ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line 1 24
 no exec
 exec-timeout 0 0
 autoselect during-login
 autoselect ppp
 script dialer cisco-default
 login local
 modem InOut
 modem autoconfigure type microcom_hdms
 transport input telnet
line aux 0
line vty 0 1
 exec-timeout 60 0
 password cisco
 login
line vty 2 5
 exec-timeout 5 0
 password cisco
 login
!
end
```

Cisco 1604 ISDN Router Configuration Without Dialer Profiles

The following configuration runs on the remote office Cisco 1604 router, which dials in to the Cisco AS5300 access server at headquarters in Figure 3. This configuration does not receive calls from the Cisco AS5300 access server.

```
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname isdn1
!
enable password cisco
!
username 5300 password cisco
username isdn1 password cisco
isdn switch-type basic-5ess
!
interface Ethernet0
 ip address 172.18.40.1 255.255.255.0
!
interface BRI0
 ip address 172.18.38.131 255.255.255.128
 encapsulation ppp
 dialer map ip 172.18.38.130 name 5300 14085269328
 dialer-group 1
 ppp authentication chap pap
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.38.130
dialer-list 1 protocol ip permit
!
line con 0
line vty 0 4
 password cisco
 login
 password cisco
 login
!
end
```

Cisco 1604 Router Asynchronous Configuration Without Dialer Profiles

The following asynchronous configuration runs on the remote office Cisco 1604 router, which dials in to the Cisco AS5300 access server at headquarters in Figure 3. This configuration does not receive calls from the Cisco AS5300 access server.

```
version xx.x
service udp-small-servers
service tcp-small-servers
!
hostname async1
!
enable password cisco
!
username 5300 password cisco
username async1 password cisco
chat script dial_out ““ “ATDT\T” timeout 60 connect \c
!
interface Ethernet0
 ip address 172.18.41.1 255.255.255.0
```

```
!
interface serial 0
 physical-layer async
 ip address 172.18.38.41 255.255.255.128
 encapsulation ppp
 dialer in-band
 dialer map ip 172.18.38.40 name 5300 modem-script dial_out 14085559328
 dialer-group 1
 ppp authentication chap pap
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.38.40
dialer-list 1 protocol ip permit
!
line con 0
line 1
 password cisco
 login
 password cisco
 login
!
end
```

Large-Scale Dial-In Configuration Using Virtual Profiles

The following example is used on each central site stack member shown in Figure 5. This configuration is for a large-scale dial-in scenario.

```
aaa new-model
aaa authentication login default none
aaa authentication ppp default radius
aaa authentication ppp admin local
aaa authorization network radius
isdn switch-type primary-5ess
!
interface Serial0:23
 no ip address
 no ip mroute-cache
 no cdp enable
 ppp authentication chap
!
tacacs-server host 172.18.203.45
virtual-profile aaa
```

The following example configures an entry running on a RADIUS security server, which is queried by each central site stack member when a call comes in. This entry includes the virtual profile configuration information for remote users dialing in to the central site stack solution.

In this example, virtual profiles are configured by both virtual templates and AAA configuration. John and Rick can dial in from anywhere and have their same keepalive settings and their own IP addresses.

The remaining attribute-value pair settings are not used by virtual profiles. They are the network-protocol access lists and route filters used by AAA-based per-user configuration.

In the AAA configuration cisco-avpair lines, “\n” is used to indicate the start of a new Cisco IOS command line.

```
john Password = “welcome”
     User-Service-Type = Framed-User,
     Framed-Protocol = PPP,
        cisco-avpair = “lcp:interface-config=keepalive 75\nip address 100.100.100.100
255.255.255.0”,
        cisco-avpair = “ip:rte-fltr-out#0=router igrp 60”,
        cisco-avpair = “ip:rte-fltr-out#3=deny 171.0.0.0 0.255.255.255”,
        cisco-avpair = “ip:rte-fltr-out#4=deny 172.0.0.0 0.255.255.255”,
        cisco-avpair = “ip:rte-fltr-out#5=permit any”
rick Password = “emoclew”
     User-Service-Type = Framed-User,
     Framed-Protocol = PPP,
        cisco-avpair = “lcp:interface-config=keepalive 100\nip address 200.200.200.200 
255.255.255.0”,
        cisco-avpair = “ip:inacl#3=permit ip any any precedence immediate”,
        cisco-avpair = “ip:inacl#4=deny igrp 0.0.1.2 255.255.0.0 any”,
        cisco-avpair = “ip:outacl#2=permit ip any any precedence immediate”,
        cisco-avpair = “ip:outacl#3=deny igrp 0.0.9.10 255.255.0.0 any”
```

Telecommuters Dialing In to a Mixed Protocol Environment

The scenario in this section describes how to provide remote access to employees who dial in to a mixed protocol enterprise network. The sample configurations provided in this section assume that enterprise telecommuters are dialing in with modems or terminal adapters from outside the LAN at headquarters.

The following sections are provided:

- Description
- Enterprise Network Topology
- Mixed Protocol Dial-In Scenarios

Description

Sometimes an enterprise conducts its daily business operations across internal mixed protocol environments. (See Figure 7 and Table 1.) For example, an enterprise might deploy an IP base across the entire intranet while still allowing file sharing with other protocols such as AppleTalk and AppleTalk Remote Access (ARA).

Figure 7 Large Enterprise with a Multiprotocol Network

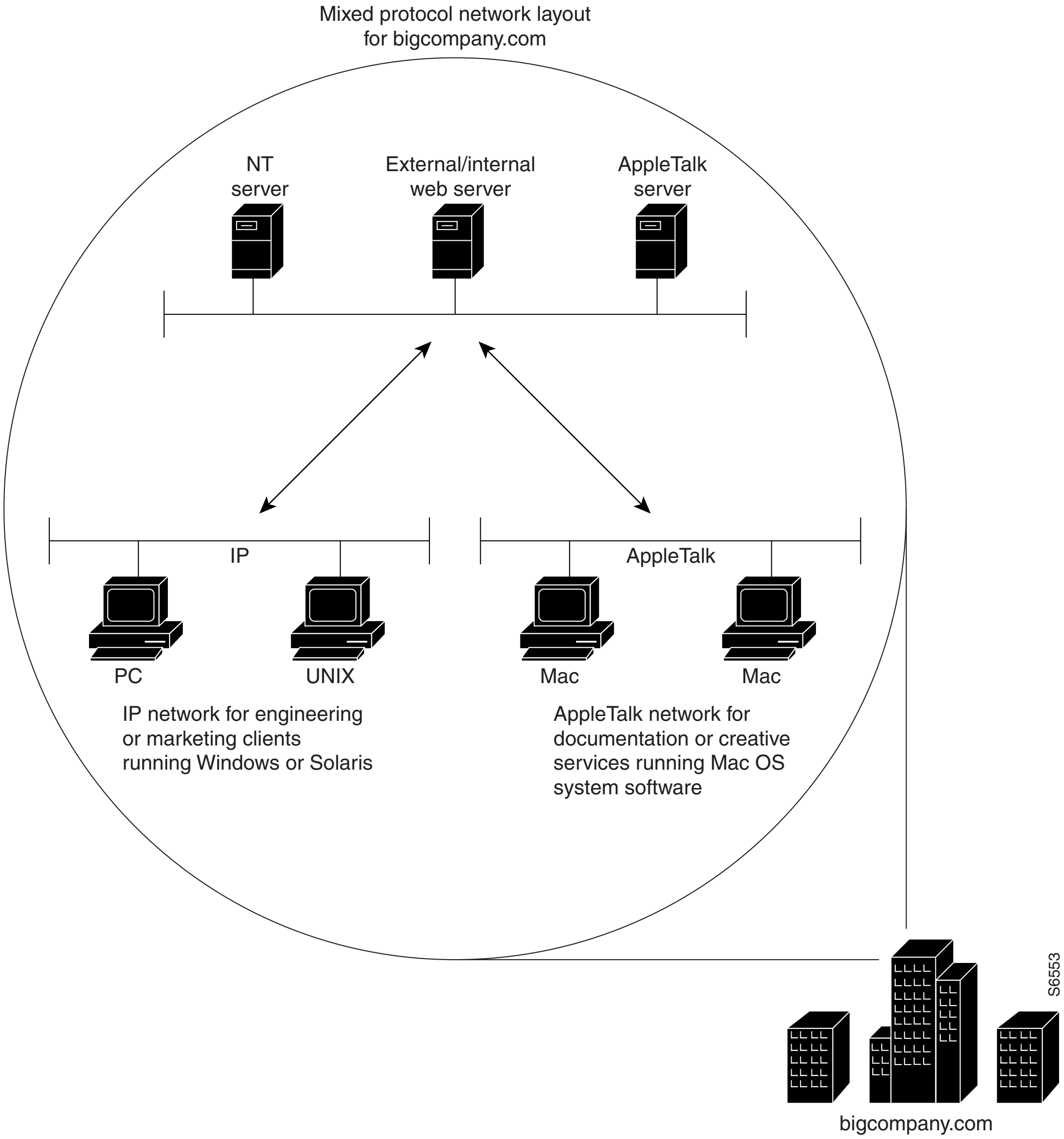


Table 1 Typical Mixed Protocol Environment

Applications Running on the Network Server	Remote or Local Client Applications	Protocol Used to Support the Network	Internal Supporting Department
Windows NT	Windows 95 or Windows 3.1 running on PCs	IP	Marketing, human resources, engineering, and customer support
UNIX	SunOS or Solaris running on a UNIX-based workstation or NCD	IP	Engineering and customer support

Table 1 Typical Mixed Protocol Environment (continued)

Applications Running on the Network Server	Remote or Local Client Applications	Protocol Used to Support the Network	Internal Supporting Department
AppleTalk	Mac OS System Software 7.5 running on Macintosh computers	AppleTalk	Documentation and creative services
NetWare	Novell NetWare client software	IPX	Marketing, and human resources, engineering, customer support

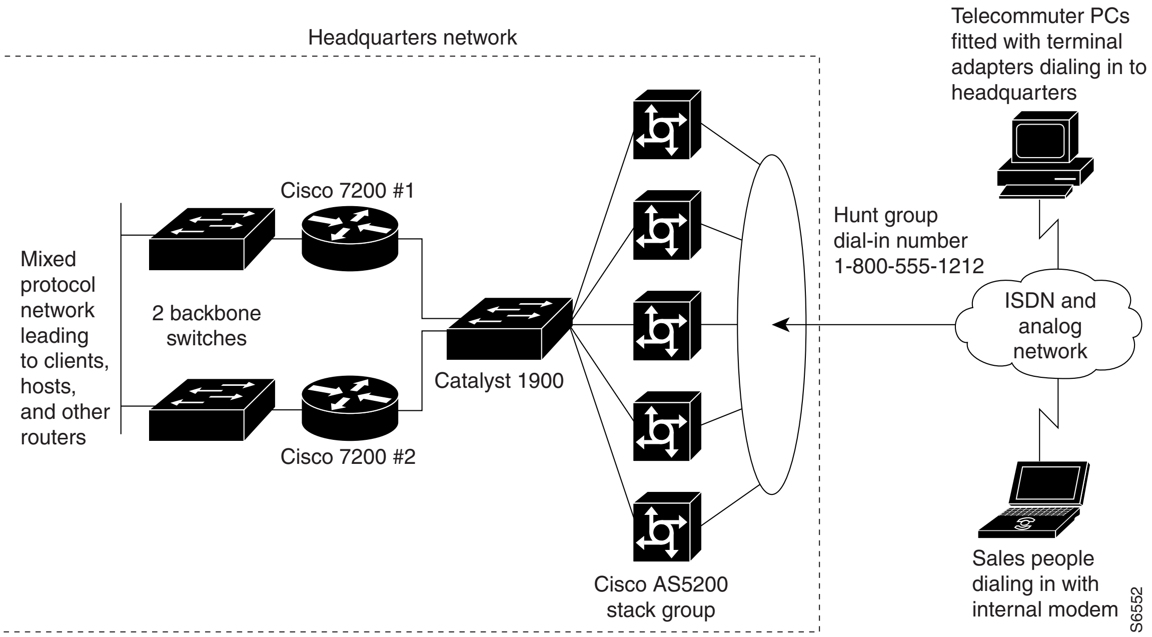
Enterprise Network Topology

Figure 8 shows a sample enterprise network, which supports 10,000 registered token card holders. Some registered users might use their access privileges each day, while others might use their access privileges very infrequently, such as only on business trips. The dial-in access provisioned for outsiders, such as partners or vendors, is supported separately in a firewalled setup.

Five Cisco AS5300 access servers are positioned to provide 250 dial-in ports for incoming modem calls. A Catalyst 1900 is used as a standalone switch to provide Ethernet switching between the Cisco AS5300 access servers and the 100BASET interfaces on the backbone routers. Two Cisco 7200 series routers are used to reduce the processing workload on the access servers and provide access to the company’s backbone. If the Cisco 7200 series routers were not used in the network solution, the Cisco AS5300 access servers could not update routing tables, especially if 20 to 30 additional routers existed on the company’s backbone. Two additional backbone switches are used to provide access to the company network.

Note Depending on your networking needs, the Cisco 7200 series routers could be substituted by one or more Cisco 3640 series routers. Additionally, the Cisco AS5300 access servers could be replaced by Cisco 3640 routers loaded with MICA digital modem cards.

Figure 8 Sample Enterprise Network Topology


Headquarters network
Telecommuter PCs fitted with terminal adapters dialing in to headquarters
Cisco 7200 #1
Mixed protocol network leading to clients, hosts, and other routers
2 backbone switches
Catalyst 1900
Cisco 7200 #2
Hunt group dial-in number 1-800-555-1212
ISDN and analog network
Cisco AS5200 stack group
Sales people dialing in with internal modem
S6552

If you are setting up dial-in access for remote terminal adapters, the settings configured on the terminal adapters must match the setting on the access server or router. Depending on your business application, terminal adapters can operate in many different modes. (See Table 2.)

Table 2 Options for Terminal Adapter Settings

Terminal Adapter Mode	Comments
Synchronous PPP	We recommend you use this mode for most terminal adapter scenarios. By default, Cisco access servers and routers have synchronous PPP enabled. Therefore, additional configuration is not required on the router or access server.
V.120	Use this mode for asynchronous to synchronous communication, which can be used to tunnel character mode sessions over synchronous ISDN. We recommend you use this mode with midrange routers, such as the Cisco 4500 series router.
V.110	Use this modem for setting up cellular modem access.

Mixed Protocol Dial-In Scenarios

The examples in the following sections are intended to run on each network device featured in Figure 8, which allows remote users to dial in to a mixed protocol environment:

- Cisco 7200 #1 Backbone Router
- Cisco 7200 #2 Backbone Router
- Cisco AS5300 Universal Access Server

Note Be sure to include your own IP addresses, host names, and security passwords where appropriate.

Cisco 7200 #1 Backbone Router

The following configuration runs on the router labeled Cisco 7200 #1 in Figure 8. Fast Ethernet interface 0/0 connects to the corporate backbone switch. Fast Ethernet interface 1/0 connects to the Catalyst 1900 switch, which in turn connects to the Cisco AS5300 access servers.

```
version xx.x
no service udp-small-servers
no service tcp-small-servers
!
hostname bbone-dial1
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
!
username admin password cisco
!
boot system flash slot0:
enable secret <password>
appletalk routing
ipx routing
!
interface FastEthernet0/0
 ip address 10.0.1.52 255.255.255.192
 appletalk cable-range 1000-1000
 appletalk zone Networking Infrastructure
 ipx network 1000
!
interface FastEthernet1/0
 ip address 10.1.1.2 255.255.255.224
 no ip redirects
 appletalk cable-range 7650-7650 7650.1
 appletalk zone Dial-Up Net
 ipx network 7650
!
 standby ip 10.1.1.1
 standby priority 101
 standby preempt
!
router eigrp 109
 redistribute static
 network 10.0.0.0
 no auto-summary
!
ip classless
ip http server
no logging console
!
ip route 10.1.2.0 255.255.255.192 10.1.1.10
!
line con 0
login authentication console
!
line vty 0 4
 login authentication default
end
```

Cisco 7200 #2 Backbone Router

The following configuration runs on the router labeled Cisco 7200 #2 in Figure 8. Fast Ethernet interface 0/0 connects to the corporate backbone switch. Fast Ethernet interface 1/0 connects to the Catalyst 1900 switch, which in turn connects to the Cisco AS5300 access servers.

```
version xx.x
no service udp-small-servers
no service tcp-small-servers
!
hostname bbone-dial2
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
!
username admin password cisco
!
boot system flash slot0:
enable secret <password>
appletalk routing
ipx routing
!
interface FastEthernet0/0
 ip address 10.0.1.116 255.255.255.192
 appletalk cable-range 1001-1001
 appletalk zone Networking Infrastructure
 ipx network 1001
!
interface FastEthernet1/0
 ip address 10.1.1.3 255.255.255.224
 no ip redirects
 appletalk cable-range 7650-7650 7650.2
 appletalk zone Dial-Up Net
 ipx network 7650
!
 standby ip 10.1.1.1
!
router eigrp 109
 redistribute static
 network 10.0.0.0
 no auto-summary
!
ip classless
ip http server
no logging console
!
ip route 10.1.2.0 255.255.255.192 10.1.1.10
!
line con 0
login authentication console
!
line vty 0 4
 login authentication console
!
end 4
```

Cisco AS5300 Universal Access Server

The following configuration runs on each Cisco AS5300 access server in the stack group shown in Figure 8:

```
version xx.x
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
appletalk routing
ipx routing
appletalk virtual net 7651 Dial-Up Net
arap network 7652 Dial-Up Net
!
hostname NAS
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin local
aaa authentication ppp default local
aaa authentication ppp dialin if-needed local
aaa authentication arap default auth-guest local
enable secret cisco
!
username admin password cisco
username pcuser1 password mypass
isdn switch-type primary-5ess
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary
 linecode b8zs
 pri-group timeslots 1-24
!
interface loopback 0
 ip address 10.1.2.0 255.255.255.192
 ipx network 7651
!
interface Ethernet0
 ip address 10.1.1.10 255.255.255.0
 appletalk cable-range 7650
 appletalk zone Dial-Up-Net
 ipx network 7650
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface Serial0:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Serial1:23
 no ip address
 encapsulation ppp
 isdn incoming-voice modem
 dialer rotary-group 0
 dialer-group 1
 no fair-queue
 no cdp enable
!
interface Group-Async1
 ip unnumbered Ethernet0
 encapsulation ppp
 async mode interactive
 peer default ip address pool dialin_pool
 appletalk client-mode
 ipx ppp-client
 no cdp enable
 ppp authentication chap pap dialin
 group-range 1 48
!
interface Dialer0
 ip unnumbered Ethernet0
 no ip mroute-cache
 encapsulation ppp
 peer default ip address pool dialin_pool
 ipx ppp-client
 appletalk client-mode
 dialer in-band
 dialer-group 1
 no fair-queue
 no cdp enable
 ppp authentication chap pap dialin
 ppp multilink
!
ip local pool dialin_pool 10.1.2.1 10.1.2.62
ip default-gateway 10.1.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
dialer-list 1 protocol ip permit
!
async-bootp dns-server 10.1.0.40 10.1.0.170
async-bootp nbns-server 10.0.235.228 10.0.235.229
!
xremote buffersize 72000
xremote tftp host 10.0.2.74
!
```

```
line con 0
 login authentication console
line 1 48
 autoselect ppp
 autoselect during-login
 autoselect arap
 arap enable
 arap authentication default
 arap timelimit 240
 arap warningtime 15
 login authentication dialin
 modem DialIn
 terminal-type dialup
line aux 0
 login authentication console
line vty 0 4
 login authentication vty
 transport input telnet rlogin
!
end
```

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.