

# Service Provider Dial Scenarios and Configurations

---

This chapter provides sample hardware and software configurations for specific dial scenarios used by service providers. Each configuration is designed to enable IP network traffic with basic security authentication.

The following scenarios are described:

- Scenario 1—Remote PCs Dialing In to a Small to Medium Scale Dial-In Solution
- Scenario 2—Remote PCs Dialing In to a Large Scale Dial-In Solution
- Scenario 3—Remote PCs Placing PPP Calls over X.25 Networks
- Scenario 4—Remote PCs Dialing In to a Virtual Private Dial Network

---

**Note** In many of these example scenarios, you can replace the Cisco AS5200 access server with a Cisco AS5300 access server. This hardware exchange provides higher call density performance and increases the number of PRI interfaces and modem ports on each chassis.

---

## Remote PCs Dialing In to a Small to Medium Scale Dial-In Solution

Many small to medium sized Internet service providers (ISPs) configure one or two access servers to provide dial-in access for their customers. Many of these dial-in customers use individual remote PCs that are not connected to local-area networks (LANs). Using an Internet access application such as Windows 95, remote clients initiate analog or digital connections using modems or home office terminal adapters.

This section provides three types of single user dial-in scenarios for ISPs plus a recommended client setup for Windows 95:

- Configuring Dial for Individual Remote PCs Using Modems
- Configuring Dial for Individual PCs Using Terminal Adapters
- Configuring Dial for a Mixture of Digital and Analog Incoming Calls
- Setting Up Windows 95 on the Remote PC Side of the Connection

---

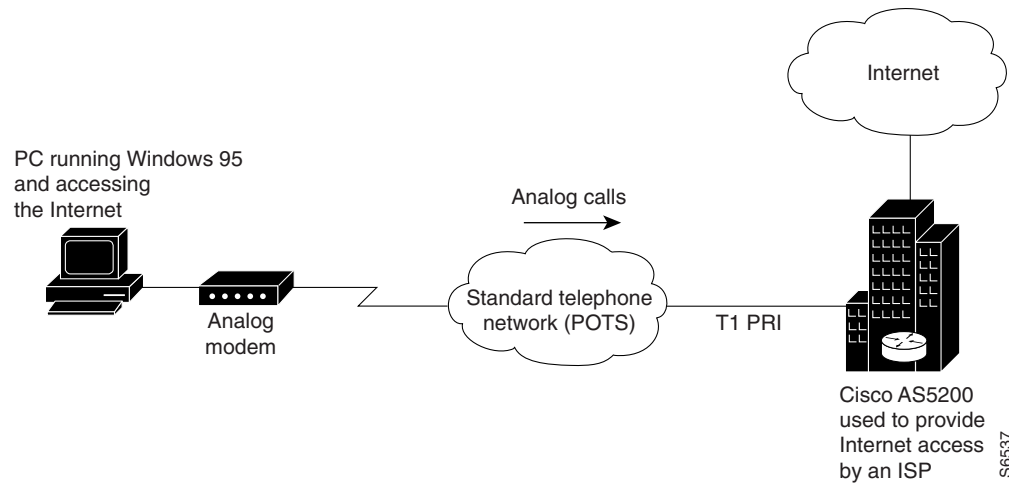
**Note** Be sure to include your own IP addresses, host names, and security passwords where appropriate. The following sample configurations assume that the dial-in clients are individual PCs running PPP, connecting to an IP network, and requiring only basic security authentication.

---

## Configuring Dial for Individual Remote PCs Using Modems

ISPs can configure a single Cisco AS5200 to receive analog calls from remote PCs connected to modems, as shown in Figure 7. The point of presence (POP) at the ISP central site could also be a Cisco 2511 access server connected to external modems.

**Figure 7 Remote PC Using an Analog Modem to Dial In to a Cisco AS5200**



## Modem Calls over ISDN PRI Configuration for the Cisco AS5200 Access Server

The following sample configuration runs on the Cisco AS5200, as shown in Figure 7, which enables remote analog users to dial in and surf the Internet:

```
!  
version 11.2  
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  
!  
interface Serial1:23  
    no ip address  
    isdn incoming-voice modem  
!  
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  
!  
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 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
```

Some service providers use a remote TACACS+ or RADIUS security server in this dial-in scenario. The following example shows a TACACS+ entry that appears in a remote security server's configuration file.

```
user = PCuser1 {
    login = cleartext "dialpass1"
    chap = cleartext "dialpass1"
    service = ppp protocol = ip {
        addr-pool = dialin_pool
    }
    service = exec {
        autocmd = "ppp negotiate"
    }
}

user = PCuser2 {
    login = cleartext "dialpass2"
    chap = cleartext "dialpass2"
    service = ppp protocol = ip {
        addr-pool = dialin_pool
    }
    service = exec {
        autocmd = "ppp negotiate"
    }
}

user = PCuser3 {
    login = cleartext "dialpass3"
    chap = cleartext "dialpass3"
    service = ppp protocol = ip {
        addr-pool = dialin_pool
    }
    service = exec {
        autocmd = "ppp negotiate"
    }
}
```

### Modem Dial-In Configuration for Robbed Bit Signaling

The following configuration is for a single Cisco AS5200 to support remote client PCs dialing in with analog modems over T1 lines. Digital ISDN calls do not transmit across these older types of channelized lines. The configuration assumes that the client can dial in and connect to the router in either terminal emulation mode (text only) or PPP packet mode.

---

**Note** The following configuration works only for analog modem calls. It includes no serial D channel configuration (Serial 0:23 and Serial 1:23). The next ISDN PRI example is for digital calls.

---

```
!
version 11.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
```

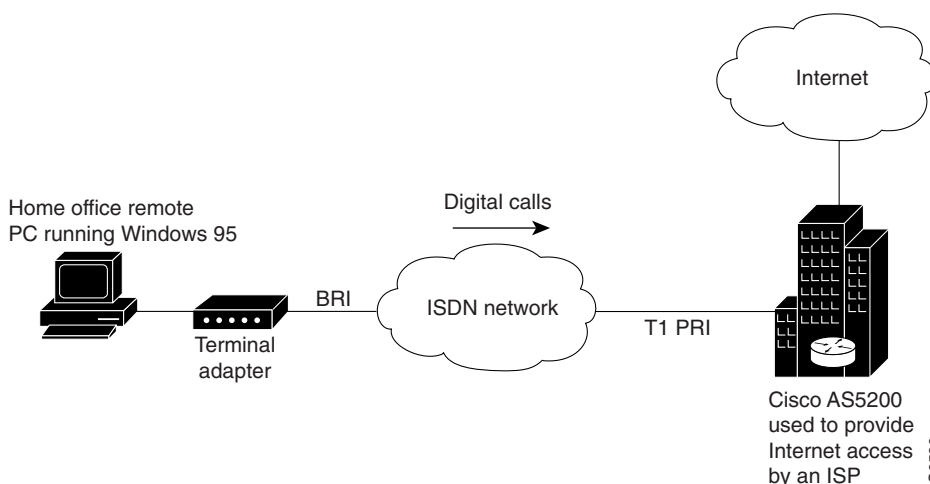
```
!  
hostname NAS  
!  
aaa new-model  
aaa authentication login console enable  
aaa authentication login vty tacacs+  
aaa authentication login dialin tacacs+  
aaa authentication ppp default tacacs+  
aaa authentication ppp dialin if-needed tacacs+  
enable secret cisco  
!  
async-bootp dns-server 10.1.3.1 10.1.3.2  
isdn switch-type primary-5ess  
!  
controller T1 0  
    framing esf  
    clock source line primary  
    linecode b8zs  
    cas-group 0 timeslots 1-24 type e&m-fgb  
!  
controller T1 1  
    framing esf  
    clock source line secondary  
    linecode b8zs  
    cas-group 0 timeslots 1-24 type e&m-fgb  
!  
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 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  
!  
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 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
```

### Configuring Dial for Individual PCs Using Terminal Adapters

ISPs can configure a single Cisco AS5200 to receive digital multilink calls from remote PCs connected to terminal adapters, as shown in Figure 8. The point of presence at the ISP's central site can be any Cisco router that supports ISDN PRI, such as the Cisco 4700-M loaded with a channelized T1 PRI network module.

**Figure 8 Remote PC Using a Terminal Adapter to Dial In to a Cisco AS5200**



To configure one Cisco AS5200 to accept both incoming ISDN and analog calls from individual terminal adapters and modems, refer to the section “Configuring Dial for a Mixture of Digital and Analog Incoming Calls.”

## ISDN PRI Dial-In Configuration for the Cisco AS5200 Access Server

The following example configures a Cisco AS5200 to enable PCs fitted with internal or external terminal adaptors to dial in to an IP network. The terminal adapter configuration is set up for asynchronous to synchronous PPP conversion. In some cases, PPP authentication must be setup for the Password Authentication Protocol (PAP) because some terminal adapters only support PAP authentication.

```
!  
version 11.2  
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  
dialer rotary-group 0  
dialer-group 1  
no fair-queue  
no cdp enable
```

## Remote PCs Dialing In to a Small to Medium Scale Dial-In Solution

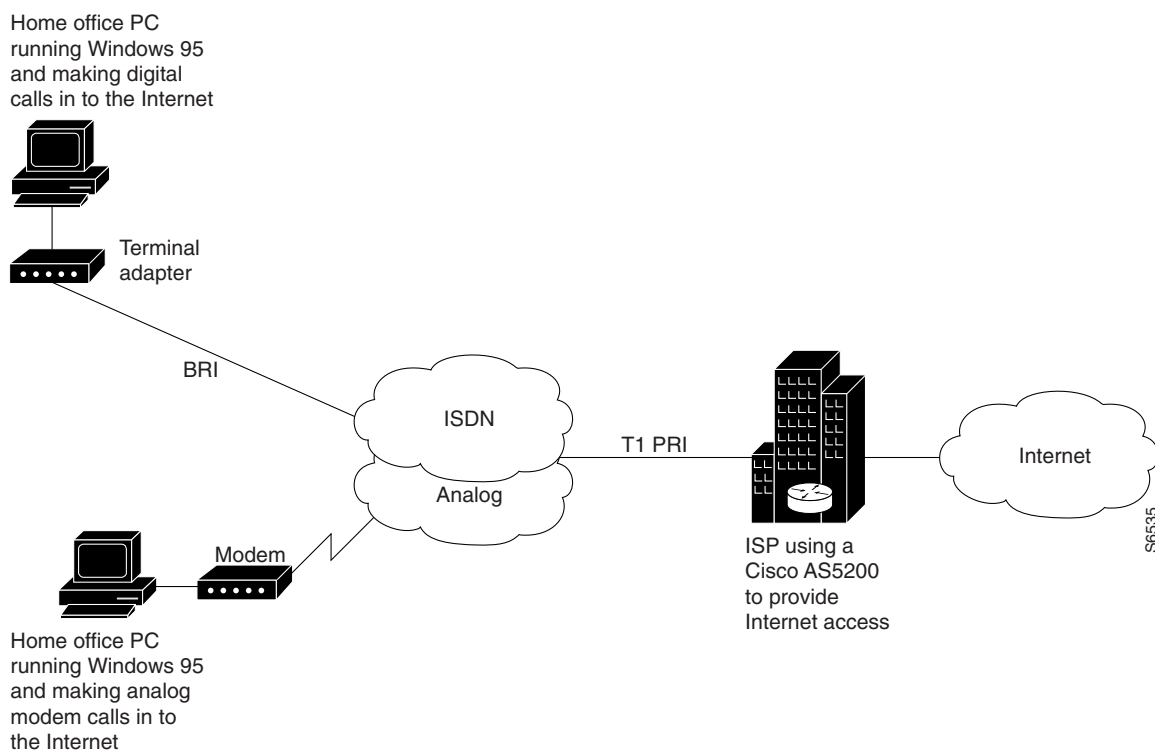
---

```
!
interface Serial1:23
  no ip address
  encapsulation ppp
  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
  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
```

## Configuring Dial for a Mixture of Digital and Analog Incoming Calls

ISPs can configure a single Cisco AS5200 to receive calls from a mixture of remote PCs connected to terminal adapters and modems, as shown in Figure 9. In this scenario, the Cisco AS5200 is used as a hybrid access server, which is its primary network application.

**Figure 9 Remote PCs Making Digital Calls and Analog Calls to a Cisco AS5200**



## Modem and ISDN Dial-In Configuration for the Cisco AS5200 Access Server

The following configuration is a combination of the modem and ISDN dial-in configurations. The incoming ISDN calls carry information about whether they are data or voice, using the bearer capability information element in the call setup packet. After the call enters the access server, it is routed either to the serial configuration or to the modems and group asynchronous configuration.

---

**Note** This configuration assumes that only individual remote PCs are dialing in; no remote routers are dialing in. For a remote router dial-in configuration, refer to the chapter “Enterprise Dial Scenarios and Configurations.”

---

```

!
version 11.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!

```

## Remote PCs Dialing In to a Small to Medium Scale Dial-In Solution

---

```
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
 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
```

## Setting Up Windows 95 on the Remote PC Side of the Connection

This section describes how to install and configure Windows 95 client software to dial in to and access network resources through a Cisco access server.

This configuration procedure is intended only as a starting point. Because Cisco does not control the design and development efforts of other companies, the configuration requirements can change without notice. This configuration information is only one of many ways of configuring a Windows 95 client application for dial-in using PPP. To set up the built-in PPP application in Windows 95 to access the ISP's IP or NetBEUI network resources, perform the following steps:

**Step 1** Double-click on the My Computer icon located either in the Applications window or on the desktop.

The My Computer window appears.

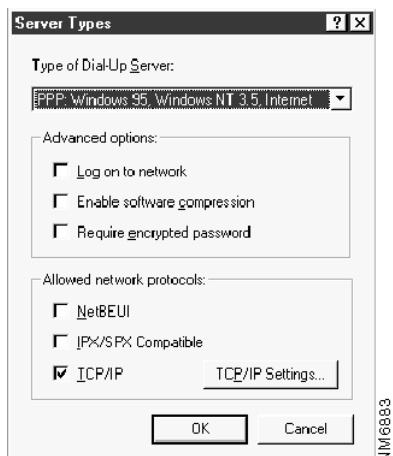
**Step 2** If you are making a connection for the first time, double-click on the Make a New Connection icon. If you have already configured your connection profiles, additional icons appear in this window, and you can double-click on them for use in the future.

- Step 3** Give the connection session a name, such as MyConnection.
- Step 4** From the list of modems, select the type of modem connected to your PC (or built in to the PC).
- Step 5** When the dialog box appears, click on the **Configure** button.  
The General, Connection, and Options folders appear stacked on top of each another. You can select each tab to configure the appropriate parameters.
- Step 6** Select the Connection tab. In the Connection folder, set data bits to 8, parity to No, and stop bits to 1. Click **Apply**.  
The Advanced Connection Settings window appears.
- Step 7** Modems usually perform all necessary data compression; however, if you have a very old modem, select Data Compression and Hardware flow control and click **OK**.
- Step 8** Select the Options tab. In the Options folder, select “Bring up terminal window after dialing” and click on the **Next** button.  
The option Bring up terminal window after dialing means that when you dial in, the access server prompts you for your username and password, then logs you in to the EXEC facility.  
A new dialog box appears that indicates you have finished configuring a dialup profile, and the “Myconnection” connectoid appears.
- Step 9** Click on the **Next** button.
- Step 10** In the Phone Number field, enter the phone number, area code, and country of the access server you intend to dial, and press Return.

You have just configured preliminary parameters to enable the Windows 95 client to dial in to an access server. You must now define additional properties:

- Step 1** Select the dialup profile connectoid. Click with the right mouse button, and pull down the menu. Select Properties.
- Step 2** In the Properties dialog box, select Server\_Type.  
The ServerTypes dialog box appears as shown in Figure 10.

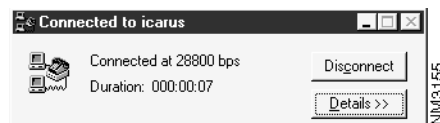
Figure 10 Windows 95 Server Types Dialog Box



- Step 3** Select PPP Windows 95 Windows NT 3.5 Internet.
- Step 4** In the Advanced options area, be sure “Log on to network” and “Enable software compression” are both disabled.
- Step 5** In the Allowed Network Protocols area, select TCP/IP if you want the PC to function as an IP client to access IP network resources.
- Step 6** Open the TCP/IP Settings pull-down menu at the bottom right corner of the dialog box by clicking on the **TCP/IP Settings** button.
- Step 7** If you are getting your addresses from a server, select Server assigned IP and Name server addresses. Otherwise, enter an IP address.
- Step 8** Select Use default gateway on remote network. Click **Apply**. Select IP compression if you intend to enable header compression of IP packets on the access server, which is enabled with the **ip tcp header-compression passive** interface configuration command.
- Step 9** Access the Control Panel, and select Internet.
- Step 10** If your PPP connection is the only modem or ISDN connection to the Internet, check the AutoDial checkbox. Uncheck this box if you have more than one outgoing connection.
- Step 11** Select MyConnection and click on the **Apply** button.

When you start an application that requires network access, you are prompted for a username and password. This username and password must match the username and password on the access server. When you select Connect, the client dials the number you entered. In a status box, you can see the information *dialing, verifying username/password*, and the dial-in application should run without problems. Figure 11 shows a successful connection.

**Figure 11 Windows 95 Connection Status Box**



## Remote PCs Dialing In to a Large Scale Dial-In Solution

Because of the significant increase in demand for Internet access, large scale dial-in solutions are required by many Internet service providers. Internet access configurations can be setup to enable users dialing in with individual computers to make mixed ISDN multilink or modem connections using a stack of Cisco AS5200 universal access servers running Multichassis Multilink PPP (MMP).

You must consider scalability and call density issues when designing a large scale dial-in scenario. Because access servers have physical limitations, such as how many dial-in users can be supported on one device, you should consider the conditions and recommendations described in Table 1.

**Table 1 Recommended Configurations for Different Remote Access Needs**

Dial-in Demand You Need to Support	Recommended Configuration
PCs dialing in, 75 to 90% modem calls, 10 to 25% ISDN calls (terminal adapters or routers), and support for less than 96 (T1) to 116 (E1) simultaneous dial-in connections.	Two Cisco AS5200s configured for IP, basic security, MMP, L2F, and no offload server.
PCs dialing in, less than 50% modem calls, more than 50% ISDN calls (terminal adapters or routers), dial-in only, and 250 or more simultaneous links into the offload server.	Three or more Cisco AS5200s configured for IP, remote security, MMP, and L2F. Each Cisco AS5200 is configured to offload its segmentation and reassembly of the multilink sessions onto an offload server, such as a Cisco 7202 or Cisco 4700.

**Note** In many of these example scenarios, you can replace the Cisco AS5200 access server with a Cisco AS5300 access server. This hardware exchange provides higher call density performance and increases the number of PRI interfaces and modem ports on each chassis.

The Cisco AccessPath Integrated Access System is an excellent solution designed to meet the demands of rapidly growing ISPs, telecommunication carriers, and other network service providers who offer managed Internet services. This universal connection server family also provides a ready solution for large enterprises as they expand their intranet requirements to include significant components of dial access.

### How a Large Scale Dial-in Solution Works

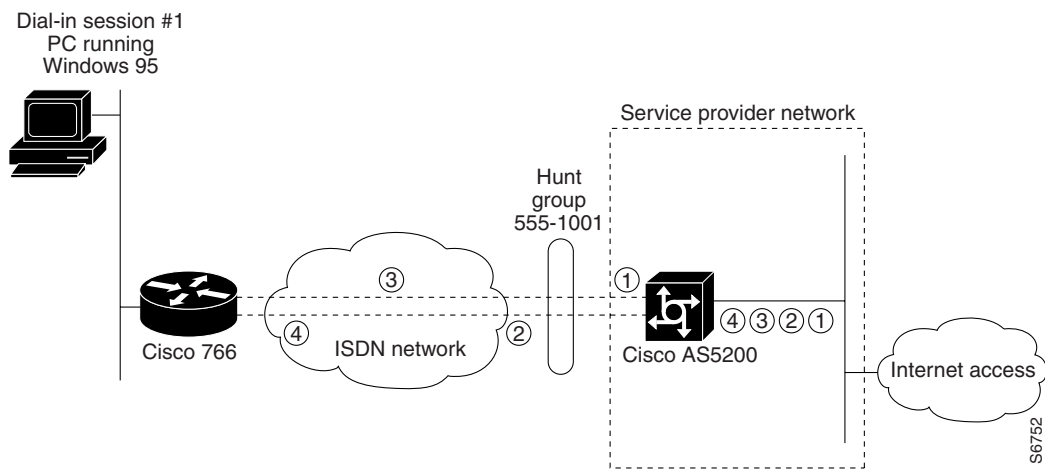
Before you configure a stack of Cisco AS5200s for large-scale dial-in access, it is useful to understand the reasons why you would need to configure this setup. This section describes the following basic concepts and how they work together in a large scale dial-in scenario:

- A Typical Multilink PPP Session
- Using Multichassis Multilink PPP
- Setting Up an Offload Server
- Using the Stack Group Bidding Protocol
- Using Layer 2 Forwarding

## A Typical Multilink PPP Session

A basic multilink session is an ISDN connection between two routing devices, such as a Cisco 766 and a Cisco AS5200. Figure 12 shows a remote PC connecting to a Cisco 766 ISDN router, which in turn opens two B-channel connections at 128 kbps across an ISDN network. The multilink PPP session is brought up. The Cisco 766 sends four packets across the network to the Cisco AS5200, which in turn reassembles the packets into the correct order and sends them out the LAN port to the Internet.

**Figure 12 A Typical Multilink PPP Session**

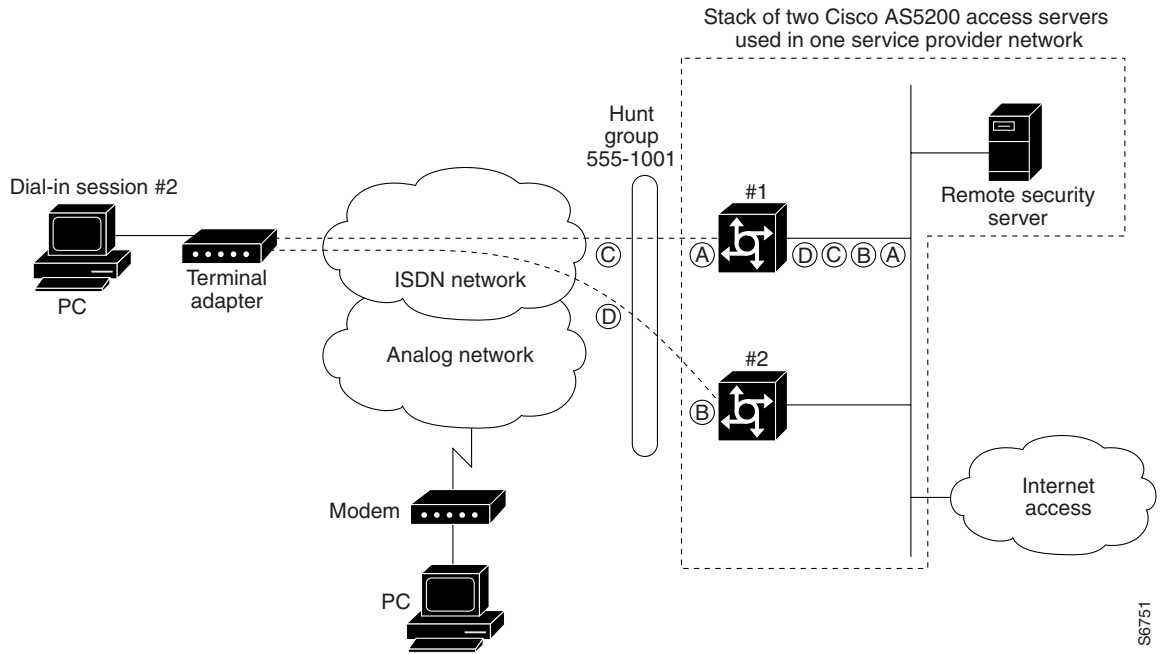


## Using Multichassis Multilink PPP

The dial solution becomes more complex when the scenario is scaled to include multiple multilink calls connecting across multiple chassis. Figure 13 shows a terminal adapter making a call in to the Cisco AS5200, labeled #1. However, only one of the access server's 46-B channels is available to accept the call. The other channels are busy with calls. The result is that one of the terminal adapter's two B-channels is redirected to device #2. At this point, a multilink multichassis session is shared between two Cisco AS5200s that belong to the same stack group. Packet fragments A and C go to device #1. Packet fragments B and D go to device #2.

Because device #1 is the first access server to receive a packet and establish a link, this access server creates a virtual interface and becomes the bundlemaster. The bundlemaster takes ownership of the multilink PPP session with the remote device. The Multichassis Multilink PPP protocol forwards the second link from device #2 to the bundlemaster, which in turn bundles the two B channels together and provides 128 kbps to the end user. Layer 2 forwarding (L2F) is the mechanism that device #2 uses to forward all packet fragments received from the terminal adapter to device #1. In this way, all packets and calls virtually appear to terminate at device #1.

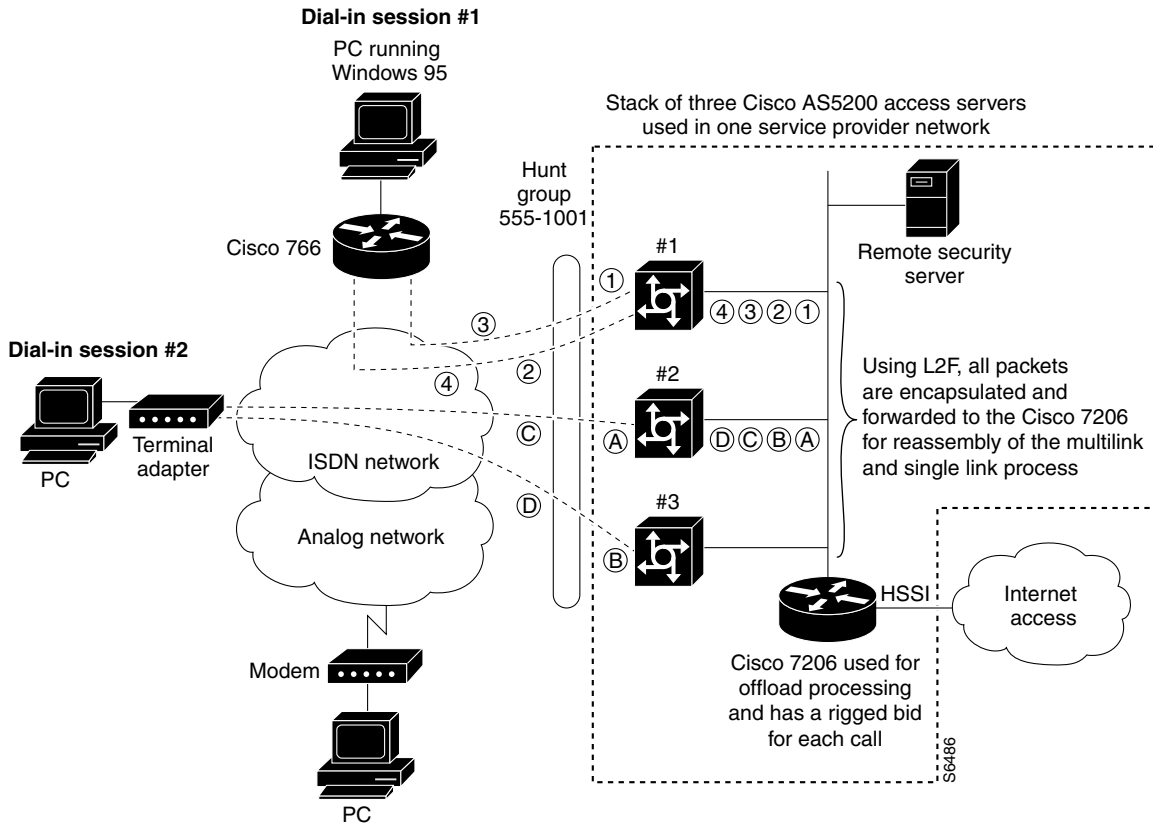
Figure 13 A Stackgroup of Access Servers Using MMP without an Offload Processor



### Setting Up an Offload Server

Because MMP is a processor-intensive application, you might need to offload the processing or segmentation and reassembly from the Cisco AS5200s to a router with a higher CPU, such as the Cisco 4700-M or Cisco 7206. We recommend you include an offload server for dial-in solutions that support more than 50% ISDN calls or more than 10 multilink sessions per Cisco AS5200. (See Figure 14.)

Figure 14 A Stack Group of Access Servers Using MMP with an Offload Processor



### Using the Stack Group Bidding Protocol

The Stack Group Bidding Protocol (SGBP) is a critical component used in multichassis multilink sessions. The SGBP unites each Cisco AS5200 in a virtual stack, which enables the access servers to become virtually tied together. Each independent stack member communicates with the other members and determines which device's CPU should be in charge of running the multilink session and packet reassembly—the bundlemaster's duty. The goal of SGBP is to find a common place to forward the links and ensure that this destination has enough CPU to perform the segmentation and packet reassembly. (See Figure 14.)

When SGBP is configured on each Cisco AS5200, each access server sends out a query to each stack group member stating, for example, "I have a call coming in from walt@options.com. What is your bid for this user?" Each access server then consults the following default bidding criteria and answers the query accordingly:

- 1 Do I have an existing call or link for the user walt@options.com? If I do, then bid very high to get this second link in to me.
- 2 If I do not have an existing call for walt@options.com, then bid a value that is proportional to how much CPU I have.
- 3 How busy am I supporting other users?

---

**Note** An offload server will always serve as the bundlemaster by bidding a higher value than the other devices.

---

### Using Layer 2 Forwarding

Layer 2 forwarding (L2F) is a critical component used in multichassis multilink sessions. If an access server is not in charge of a multilink session, the access server encapsulates the fragmented PPP frames and forwards them to the bundlemaster using L2F. The master device receives the calls, not through the dial port (such as a dual T1/PRI card), but through the LAN or Ethernet port. L2F simply tunnels packet fragments to the device that owns the multilink session for the call. If you include an offload server in your dial-in scenario, it creates all the virtual interfaces, owns all the multilink sessions, and reassembles all the fragmented packets received by L2F via the other stackgroup members. (See Figure 14.)

### Large Scale Dial-In Configuration Examples

This section provides sample Cisco IOS configurations for the devices shown in Figure 14. Be sure to include your own IP addresses, passwords, or host names where applicable.

- Cisco AS5200 #1 Configuration
- Cisco AS5200 #2 Configuration
- Cisco AS5200 #3 Configuration
- Cisco 7206 Configuration
- RADIUS Remote Security Examples

---

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

---

### Cisco AS5200 #1 Configuration

The following configuration runs on the Cisco AS5200 labeled #1 in Figure 14:

```
!
version 11.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname AS5200-1
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin radius
aaa authentication ppp default local
aaa authentication ppp dialin if-needed radius
aaa authorization exec local radius
aaa authorization network radius
aaa accounting network start-stop radius
```

```
aaa accounting exec start-stop radius
enable secret cisco
!
username admin password cisco
username MYSTACK password STACK-SECRET
sgbp group MYSTACK
sgbp member AS5200-2 10.1.1.12
sgbp member AS5200-3 10.1.1.13
sgbp member 7200 10.1.1.14
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 10.1.2.62 255.255.255.192
!
interface Ethernet0
 ip address 10.1.1.11 255.255.255.0
 ip summary address eigrp 10 10.1.2.0 255.255.255.192
!
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
```

## Remote PCs Dialing In to a Large Scale Dial-In Solution

---

```
!  
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  
radius-server host 10.1.1.23 auth-port 1645 acct-port 1646  
radius-server host 10.1.1.24 auth-port 1645 acct-port 1646  
radius-server key cisco  
!  
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
```

## Cisco AS5200 #2 Configuration

The following configuration runs on the Cisco AS5200 labeled #2 in Figure 14:

```
!  
version 11.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname AS5200-2  
!  
aaa new-model  
aaa authentication login default local  
aaa authentication login console enable  
aaa authentication login vty local  
aaa authentication login dialin radius  
aaa authentication ppp default local
```

```
aaa authentication ppp dialin if-needed radius
aaa authorization exec local radius
aaa authorization network radius
aaa accounting network start-stop radius
aaa accounting exec start-stop radius
enable secret cisco
!
username admin password cisco
username MYSTACK password STACK-SECRET
sgbp group MYSTACK
sgbp member AS5200-1 10.1.1.11
sgbp member AS5200-3 10.1.1.13
sgbp member 7200 10.1.1.14
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 10.1.2.126 255.255.255.192
!
interface Ethernet0
 ip address 10.1.1.12 255.255.255.0
 ip summary address eigrp 10 10.1.2.64 255.255.255.192
!
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
```

## Remote PCs Dialing In to a Large Scale Dial-In Solution

---

```
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
no auto-summary
!
ip local pool dialin_pool 10.1.2.65 10.1.2.114
ip default-gateway 10.1.1.1
ip classless
!
dialer-list 1 protocol ip permit
radius-server host 10.1.1.23 auth-port 1645 acct-port 1646
radius-server host 10.1.1.24 auth-port 1645 acct-port 1646
radius-server key cisco
!
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
```

## Cisco AS5200 #3 Configuration

The following configuration runs on the Cisco AS5200 labeled #3 in Figure 14:

```
!
version 11.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname AS5200-3
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
```

```
aaa authentication login dialin radius
aaa authentication ppp default local
aaa authentication ppp dialin if-needed radius
aaa authorization exec local radius
aaa authorization network radius
aaa accounting network start-stop radius
aaa accounting exec start-stop radius
enable secret cisco
!
username admin password cisco
username MYSTACK password STACK-SECRET
sgbp group MYSTACK
sgbp member AS5200-1 10.1.1.11
sgbp member AS5200-2 10.1.1.12
sgbp member 7200 10.1.1.14
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 10.1.2.190 255.255.255.192
!
interface Ethernet0
  ip address 10.1.1.13 255.255.255.0
  ip summary address eigrp 10 10.1.2.128 255.255.255.192
!
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
```

## Remote PCs Dialing In to a Large Scale Dial-In Solution

---

```
!
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
 no auto-summary
!
ip local pool dialin_pool 10.1.2.129 10.1.2.178
ip default-gateway 10.1.1.1
ip classless
!
dialer-list 1 protocol ip permit
radius-server host 10.1.1.23 auth-port 1645 acct-port 1646
radius-server host 10.1.1.24 auth-port 1645 acct-port 1646
radius-server key cisco
!
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
```

## Cisco 7206 Configuration

The following configuration runs on the Cisco 7206 router shown in Figure 14.

---

**Note** Any Cisco router that has a strong CPU can be used as an offload server, such as a Cisco 4500-M, 4700-M, or 3640. However, the router must be configured to handle the necessary processing overhead demanded by each stack member.

---

```
!
version 11.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname 7200
!
aaa new-model
aaa authentication login default local
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin radius
aaa authentication ppp default local
aaa authentication ppp dialin if-needed radius
aaa authorization exec local radius
aaa authorization network radius
aaa accounting network start-stop radius
aaa accounting exec start-stop radius
enable secret cisco
!
username MYSTACK password STACK-SECRET
username admin password cisco
multilink virtual-template 1
sgbp group MYSTACK
sgbp member AS5200-1 10.1.1.11
sgbp member AS5200-2 10.1.1.12
sgbp member AS5200-3 10.1.1.13
sgbp seed-bid offload
async-bootp dns-server 10.1.3.1 10.1.3.2
!
interface Loopback0
 ip address 10.1.2.254 255.255.255.192
!
interface Ethernet2/0
 ip address 10.1.1.14 255.255.255.0
 ip summary address eigrp 10 10.1.2.192 255.255.255.192
!
interface Ethernet2/1
 no ip address
 shutdown
!
interface Ethernet2/2
 no ip address
 shutdown
!
interface Ethernet2/3
 no ip address
 shutdown
```

```
!
interface Virtual-Template1
 ip unnumbered Loopback0
 no ip mroute-cache
 peer default ip address pool dialin_pool
 ppp authentication chap pap dialin
 ppp multilink
!
router eigrp 10
 network 10.0.0.0
 passive-interface Virtual-Template1
 no auto-summary
!
ip local pool dialin_pool 10.1.2.193 10.1.2.242
ip default-gateway 10.1.1.1
ip classless
!
radius-server host 10.1.1.23 auth-port 1645 acct-port 1646
radius-server host 10.1.1.24 auth-port 1645 acct-port 1646
radius-server key cisco
!
line con 0
 login authentication console
line aux 0
 login authentication console
line vty 0 4
 login authentication vty
!
end
```

### RADIUS Remote Security Examples

The following RADIUS examples use the IETF syntax for the attributes. Depending on how the dictionary is set up, the syntax for these configurations might differ between versions of RADIUS daemons.

---

**Note** You must have the **async dynamic address** command enabled on the network access server if you use Framed-IP-Address to statically assign IP addresses.

---

#### Example 1

The following example shows a user setup for PPP. The user's IP address comes from the configured default IP address that is set up on the interface (which could be a specific default IP address, a pointer to a local pool of addresses, or a pointer to a DHCP server). The special address that signals the default address is 255.255.255.254.

```
pppme Password = "cisco"
      CHAP-Password = "cisco"
      Service-Type = Framed,
      Framed-Protocol = PPP,
      Framed-IP-Address = 255.255.255.254
```

### Example 2

The following example shows a user setup for PPP and a static IP address that stays with the user across all connections. Make sure your router is set up to support this configuration, especially for large or multiple POPs.

```
staticallypppme Password = "cisco"  
    CHAP-Password = "cisco"  
    Service-Type = Framed,  
    Framed-Protocol = PPP,  
    Framed-IP-Address = 1.1.1.1
```

### Example 3

The next example supports a router dialing in, which requires that a static IP address and a remote Ethernet interface be added to the network access server's routing table. The router's WAN port is assigned the address 1.1.1.2. The remote Ethernet interface is 2.1.1.0 with a class C mask. Be sure your routing table can support this requirement. You might need to redistribute the static route with a dynamic routing protocol.

```
routeime Password = "cisco"  
    CHAP-Password = "cisco"  
    Service-Type = Framed,  
    Framed-Protocol = PPP,  
    Framed-IP-Address = 1.1.1.1  
    Framed-Route = "2.1.1.0/24 1.1.1.2"
```

### Example 4

The following example shows a user setup for the SLIP protocol. Remote users are assigned to the default address on the interface.

```
slipme Password = "cisco"  
    Service-Type = Framed,  
    Framed-Protocol = SLIP,  
    Framed-IP-Address = 255.255.255.254
```

### Example 5

The following example shows a user setup for SLIP and a static IP address that stays with the user across all connections. Make sure your routing is set up to support this configuration, especially for large or multiple POPs.

```
staticallyslipme Password = "cisco"  
    Service-Type = Framed,  
    Framed-Protocol = SLIP,  
    Framed-IP-Address = 1.1.1.13
```

### Example 6

This example automatically Telnets the user to a UNIX host. This configuration is useful for registering new users, providing basic UNIX shell services, or providing a guest account.

```
telnetme Password = "cisco"  
    Service-Type = Login,  
    Login-Service = Telnet,  
    Login-IP-Host = 4.1.1.1
```

### Example 7

This example automatically rlogins the user to a UNIX host:

```
rloginme Password = "cisco"  
    Service-Type = Login,  
    Login-Service = Rlogin,  
    Login-IP-Host = 4.1.1.2
```

If you want to prevent a second password prompt from being brought up, you must have the following two commands enabled on the router or access server:

- **rlogin trusted-remoteuser-source local**
- **rlogin trusted-localuser-source radius**

## Remote PCs Placing PPP Calls over X.25 Networks

Remote PCs stationed in X.25 PAD networks can access the Internet by dialing in to Cisco routers, which support PPP. By positioning a Cisco router at the corner of an X.25 network, ISPs and telcos can provide Internet and PPP access to PAD users. All remote PAD users, who dial in to X.25 networks, dial in to one Cisco router that allows PPP connections. Although connection performance is not optimal, these X.25 to PPP calls utilize installed bases of X.25 equipment and cost less to operate than connecting over the standard telephone network.

---

**Note** This dial-in scenario can be used as an enterprise solution too. In this case, an enterprise consults with a third-party service provider that allows enterprises to leverage existing X.25 enterprise equipment to provide connections back into enterprise environments.

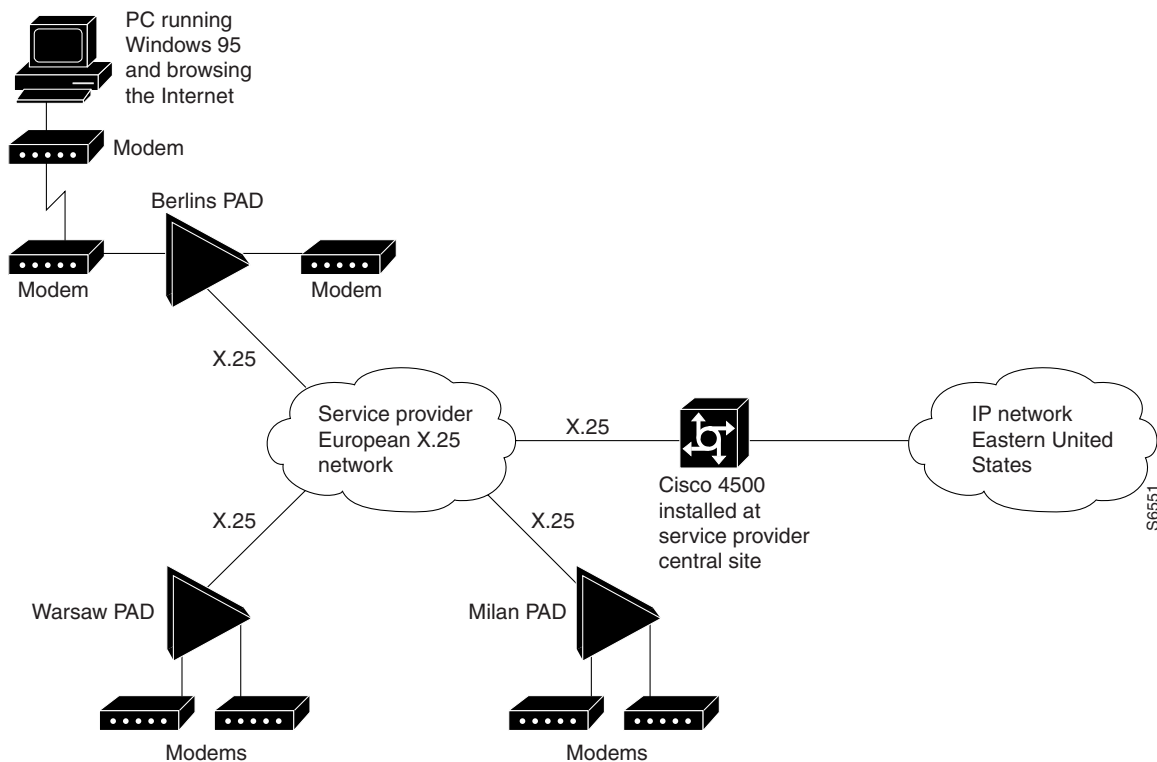
---

Many cities throughout the world have large installed bases of PCs interfacing with older modems, PADs, and X.25 networks. These remote PCs or terminals dial in to PADs and make X.25 PAD calls or terminal connections to mainframe computers or other devices, which run the X.25 protocol. Unfortunately, the user interface is only a regular text based screen in character mode (as opposed to packet mode). Therefore, many ISPs and telcos who have large investments in X.25 networks are upgrading their outdated equipment and creating separate networks for PPP connections. Because this upgrade process takes significant time and money to complete, using a Cisco router to allow PPP connections over an X.25 network is a good interim solution for a dead-end dial case.

Figure 15 shows a remote PC browsing the Internet through an X.25 PAD call and a Cisco 4500 router. This X.25 network is owned by an ISP or telco who is heavily invested in X.25 equipment, currently upgrading their outdated equipment, and creating separate networks for PPP connections. In this topology, the Cisco 4500 performs protocol translation between the protocols X.25 and PPP. The router is configured to accept an incoming X.25 PAD call, run and unpack PPP packets over the call, and enable the remote PC to function as if it were on the IP network.

For more information about configuring protocol translation, see the chapter “Configuring Protocol Translation and Virtual Asynchronous Devices.”

Figure 15 Remote PC Browsing the Internet through an X.25 PAD Call and a Cisco 4500



### Cisco AS5200 Configuration

In the following example, PAD callers, who dial 4085551234, receive a router prompt. PAD callers who dial 408555123401 start PPP and pick up an address from the IP pool called dialin\_pool. These addresses are “borrowed” from the Ethernet interface on the Cisco AS5200. Additionally, you can create a loopback interface network and set the X.25 addresses. However, be sure to run a routing protocol to advertise the loopback interface network if you use this method.

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

```

!
version 11.2
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

vty-async
vty-async ppp authentication chap pap
!
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
 encapsulation x25
 x25 address 4085551234
 x25 accept-reverse
 x25 default pad
!
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

translate x25 408555123401 ppp ip-pool scope-name dialin_pool
!
!
dialer-list 1 protocol ip permit
!
line con 0
 login authentication console
line aux 0
 login authentication console
line vty 0 150
 login authentication vty
 transport input telnet rlogin
!
end
```

## Remote PCs Dialing In to a Virtual Private Dial Network

A growing number of ISPs are providing virtual private dial networks (VPDNs) to enterprise customers, which are dial-in only solutions.

VPDN is described in the following sections:

- Benefits of VPDNs and Who Uses Them
- Choosing the Right VPDN Scenario for Your Business Application
- How a VPDN Works
- VPDN Configuration Examples with Local Security
- Large Scale VPDN Example Using a Remote RADIUS Server

### Benefits of VPDNs and Who Uses Them

VPDNs are dial-in access services provided by ISPs to enterprise customers who choose not to purchase, configure, or maintain access servers or modem pools. Using this scenario, the enterprise customer avoids costly front-end access resources (such as hundreds of modems, access servers, and additional telephone lines) as well as support and maintenance costs. The VPDN scenario is also a solution for ISPs that have excess modem capacity and want to develop and offer a value-added dial-in service to their organization. Enterprises can save on capital investment by researching whether or not their ISP provides this kind of dial service.

### Choosing the Right VPDN Scenario for Your Business Application

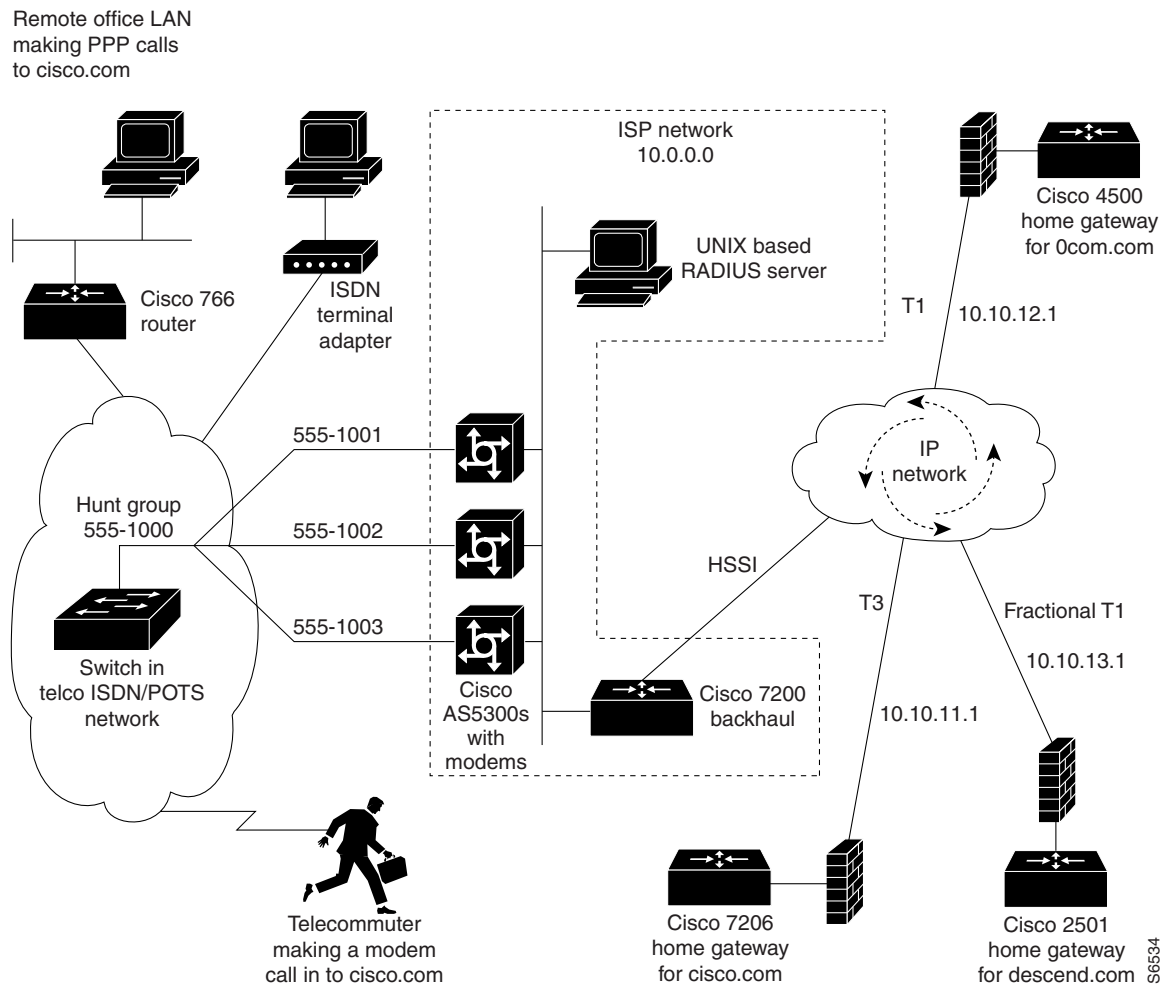
There are two scenario-based approaches used to define or set up a VPDN solution. For ISPs that provide access for five or fewer enterprises or domains, Cisco Systems recommends a small-sized VPDN with a local security solution. For ISPs that provide access for six or more enterprises or domains, Cisco Systems recommends a large-sized VPDN with a remote access control security solution. Cisco also recommends a large-scale VPDN for ISPs that have a large pool of network access servers to maintain. The appropriate solution depends primarily on serviceability and scalability issues.

The difference between a small and large VPDN is the number of high-density access servers installed at the ISP's POP in addition to local versus remote security. Small-scale VPDNs require system administrators to maintain the security database on each dial-in access server. For large scale VPDNs, the ISP's authentication process is easily maintained by a single access control security server using a UNIX-based application such as CiscoSecure. Each time a customer is added to a large-scale solution, a new domain name map entry does not need to be added locally to each access server's configuration file. Instead, the entry is recorded once in the security server's database. Remote security server solutions also take on the responsibility of defining L2F tunnel definitions and user names.

## How a VPDN Works

A sample network topology for a VPDN scenario is shown in Figure 16. An ISP has a stack of Cisco AS5200s connected to its 10.0.0.0 network, which provides a pool of integrated modems (for analog calls) and ISDN bearer channels (for digital calls) for three enterprise customers (cisco.com, Ocom.com, and descend.com). The ISP provides each enterprise with its own home gateway router, firewall setup configured for authentication, and a common dial-in telephone number for each company's group of telecommuters or remote office users. Although the ISP provides the dial-in vehicle for the remote nodes, each enterprise customer assigns its own IP addresses and processes all the PPP packets sent by the remote PCs. All network resource security is owned and maintained by the enterprise customer. From the enterprise's point of view, the connections initiated by the remote clients are virtually private and maintained by the enterprise.

**Figure 16 Network Topology for a Virtual Private Dialup Network**



All enterprise home gateways only allow incoming L2F UDP packets on the WAN connection to their service provider. This configuration effectively firewall off any IP connectivity other than that which is needed for the forwarding of user traffic. These enterprise network connections are virtually private and owned by the enterprise.

On the ISP's side of the configuration, each T1 line is assigned its own dial-in telephone number. The telco groups all T1 lines that connect to each Cisco AS5200 into a single hunt group. Because T1 lines are limited to 24 channels, the telco creates a hunt group telephone number so that the dial-in access is not limited to only 24 simultaneous users. A hunt group telephone number (shown in Figure 16 as 555-1000) provides the dial-in access for the dial-in clients. The hunt group number is the only number that clients dial in to, regardless if they are using modems, terminal adapters, or routers. As soon as a call comes into the telco's network, the telco's switch searches or hunts for the first available channel on each of the Cisco AS5200's T1 lines. One hunt group telephone number on the telco side provides multiple dial-in services for the ISP.

Depending on the size of the VPDN solution needed, local or remote security is configured on the ISP's access network. For small size VPDN solutions, the security database is configured and replicated locally on each Cisco AS5200. For larger size VPDN solutions, the security database is configured on an access control server (for example, a TACACS+ or RADIUS server running CiscoSecure). Each Cisco AS5200 that receives a call queries the local or remote security database for information about where to tunnel or send the call (for example, user name, domain mapping, home gateway address, and user profile).

Here is an example of how the VPDN dial-in process works for a telecommuter dialing in to the Cisco System's network. The telecommuter dials in to the ISP's modem pool using the hunt group dial-in number provisioned for Cisco Systems. Based on the dial-in client's login information, a Cisco AS5200 creates an L2F tunnel and relays the client's PPP frames over an IP network to the cisco.com gateway router for authentication. After a tunnel is built to the cisco.com gateway router, a backhaul router (shown in Figure 16 as the Cisco 7200) forwards encapsulated PPP frames on top of UDP packets through an IP substrate—a networking base that packets travel through.

---

**Note** Instead of basing the routing on the domain and user name, an ISP can build an L2F tunnel based on the phone number that the remote clients dial. However, this dialed number identification service (DNIS) information is collected only if you are using ISDN PRI lines, or if you have CT1 lines, and you must use MICA modem technology.

---

## VPDN Configuration Examples with Local Security

The following sample configurations run on the routers and access servers featured in Figure 16. The configurations include only basic IP and local security support.

- Cisco AS5200 Configuration for the Service Provider's Network Access Servers
- Cisco 2501 Home Gateway Configuration for descend.com
- Cisco 4500 Series Home Gateway Configuration for 0com.com
- Cisco 7206 Series Home Gateway Configuration for cisco.com

---

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

---

## Cisco AS5200 Configuration for the Service Provider's Network Access Servers

The following configuration is deployed on each of the Cisco AS5200s included in the service provider's stack group. See Figure 16. The only parts of the configuration that are configured differently on each access server are the Ethernet IP addresses and the IP addresses for the local pools.

```

!
version 11.2
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 ISP password ISP
username cisco.com password CISCO_SECRET
username 0com.com password 0COM_SECRET
username descend.com password DESCEND_SECRET
vpdn enable
vpdn outgoing cisco.com ISP ip 10.10.11.1
vpdn outgoing 0com.com ISP ip 10.10.12.1
vpdn outgoing descend.com ISP ip 10.10.13.1
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

```

## Remote PCs Dialing In to a Virtual Private Dial Network

---

```
!  
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  
  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
```

## Cisco 2501 Home Gateway Configuration for descend.com

The following configuration runs on the Cisco 2501, which is used by descend.com in Figure 16.

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname DESCEND_HGW
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
!
username descend.com password DESCEND_SECRET
username ISP password ISP
username pcuser@descend.com password cisco
vpdn enable
vpdn incoming ISP descend.com virtual-template 1
!
interface Ethernet0
  ip address 3.1.1.1 255.255.255.0
!
interface Serial0
  ip address 10.10.13.1 255.255.255.252
  ip access-group 101 in
  encapsulation ppp
!
interface Serial1
  no ip address
  shutdown
!
interface Virtual-Template1
  ip unnumbered Ethernet0
  peer default ip address pool descend-pool
  ppp authentication chap pap
!
router eigrp 3
  network 3.0.0.0
  no auto-summary
!
ip local pool descend-pool 3.1.1.3 3.1.1.22
ip classless
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

You can also use the following access lists to firewall off this home gateway from the VPDN provider. However, these access lists cut off all IP traffic on the router except for L2F information.

- **access-list 101 permit udp any host *ip-address-of-serial-interface* eq 1701**
- **access-list 101 deny ip any any**

### Cisco 4500 Series Home Gateway Configuration for Ocom.com

The following configuration runs on the Cisco 4500, which is used by Ocom.com in Figure 16.

```
!  
version 11.2  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname OCOM_HGW  
!  
aaa new-model  
aaa authentication login default local  
aaa authentication ppp default local  
!  
username Ocom.com password OCOM_SECRET  
username ISP password ISP  
username pcuser@Ocom.com password cisco  
vpdn enable  
vpdn incoming ISP Ocom.com virtual-template 1  
!  
interface Ethernet0  
 ip address 2.1.1.1 255.255.255.0  
!  
interface Ethernet1  
 no ip address  
 shutdown  
!  
interface Serial0  
 ip address 10.10.12.1 255.255.255.252  
 ip access-group 101 in  
 encapsulation ppp  
!  
interface Serial1  
 no ip address  
 shutdown  
!  
interface Serial2  
 no ip address  
 shutdown  
!  
interface Serial3  
 no ip address  
 shutdown  
!  
interface Virtual-Template1  
 ip unnumbered Ethernet0  
 peer default ip address pool Ocom-pool  
 ppp authentication chap pap  
!  
router eigrp 2  
 network 2.0.0.0  
 no auto-summary  
!  
ip local pool Ocom-pool 2.1.1.3 2.1.1.52  
ip classless  
!
```

```

!
line con 0
line aux 0
line vty 0 4

```

You can also use the following access lists to firewall off this home gateway from the VPDN provider. However, these access lists cut off all IP traffic on the router except for L2F information.

- **access-list 101 permit udp any host *ip-address-of-serial-interface* eq 1701**
- **access-list 101 deny ip any any**

## Cisco 7206 Series Home Gateway Configuration for cisco.com

The following configuration runs on the Cisco 7206, which is used by cisco.com in Figure 16.

```

!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname CISCO_HGW
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
!
username cisco.com password CISCO_SECRET
username ISP password ISP
username pcuser@cisco.com password cisco
vpdn enable
vpdn incoming ISP cisco.com virtual-template 1
!
interface Ethernet2/0
 ip address 1.1.1.1 255.255.255.0
!
interface Ethernet2/1
 no ip address
 shutdown
!
interface Ethernet2/2
 no ip address
 shutdown
!
interface Ethernet2/3
 no ip address
 shutdown
!
interface Serial3/0
 ip address 10.10.11.1 255.255.255.252
 ip access-group 101 in
 encapsulation ppp
!
interface Serial3/1
 no ip address
 shutdown
!
interface Serial3/2
 no ip address
 shutdown
!
interface Serial3/3
 no ip address
 shutdown

```

```
!  
interface Virtual-Template1  
 ip unnumbered Ethernet2/1  
 peer default ip address pool cisco-pool  
 ppp authentication chap pap  
!  
router eigrp 1  
 network 1.0.0.0  
 no auto-summary  
!  
ip local pool cisco-pool 1.1.1.3 1.1.1.102  
ip classless  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
end
```

You can also use the following access lists to firewall off this home gateway from the VPDN provider. However, these access lists cut off all IP traffic on the router except for L2F information.

- **access-list 101 permit udp any host *ip-address-of-serial-interface* eq 1701**
- **access-list 101 deny ip any any**

## Large Scale VPDN Example Using a Remote RADIUS Server

Large scale VPDNs can provide dial-in access for dozens of different home gateways owned and maintained by different customers. For these large scale scenarios, it is not practical to configure the tunneling information for each home gateway on each network access server. Instead, the call tunneling information is setup on an access control server, such as a UNIX-based RADIUS server, which is owned and maintained by the service provider. However, all network resource security is still maintained by the enterprise customers at their home gateways.

This section includes a Cisco AS5200 configuration using RADIUS security, which is deployed on each stack group member in the large scale VPDN solution. This section also includes a user's file for a UNIX-based RADIUS server, which keeps track of all the incoming call tunneling information for multiple home gateways.

To compliment a remote RADIUS security solution, run the following configuration on each Cisco AS5200 in the VPDN stack group. See Figure 16.

---

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

---

```
!  
version 11.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname ISP  
!  
aaa new-model  
aaa authentication login default local
```

```
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin radius
aaa authentication ppp default local
aaa authentication ppp dialin if-needed radius
aaa authorization network radius
aaa accounting exec start-stop radius
aaa accounting network start-stop radius
enable secret cisco
!
username admin password cisco
vpdn enable
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
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
radius-server host 10.1.1.23 auth-port 1645 acct-port 1646
radius-server host 10.1.1.24 auth-port 1645 acct-port 1646
radius-server key cisco
!
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
```

The following user's file runs on the UNIX-based RADIUS server shown in Figure 16. This user's file provides the L2F tunnel definitions and user names for ten different home gateway routers at ten different company sites. This configuration uses the `cisco-avpair` attribute, which is a vendor-specific attribute (attribute 26). The RADIUS server must support the vendor-specific option, as defined in RFC 2138. Otherwise, the configuration will not work.

```
corp1.com Password = "cisco", Service-Type = Outbound-User
cisco-avpair = "vpdn:tunnel-id=NAS",
cisco-avpair = "vpdn:nas-password=corp1secret",
cisco-avpair = "vpdn:gw-password=corp1secret",
cisco-avpair = "vpdn:ip-addresses=10.10.1.1"

corp2.com Password = "cisco", Service-Type = Outbound-User
cisco-avpair = "vpdn:tunnel-id=NAS",
cisco-avpair = "vpdn:nas-password=corp2secret",
cisco-avpair = "vpdn:gw-password=corp2secret",
cisco-avpair = "vpdn:ip-addresses=10.10.2.1"
```

```

corp3.com Password = "cisco", Service-Type = Outbound-User
      cisco-avpair = "vpdn:tunnel-id=NAS",
      cisco-avpair = "vpdn:nas-password=corp3secret",
      cisco-avpair = "vpdn:gw-password=corp3secret",
      cisco-avpair = "vpdn:ip-addresses=10.10.3.1"

corp4.com Password = "cisco", Service-Type = Outbound-User
      cisco-avpair = "vpdn:tunnel-id=NAS",
      cisco-avpair = "vpdn:nas-password=corp4secret",
      cisco-avpair = "vpdn:gw-password=corp4secret",
      cisco-avpair = "vpdn:ip-addresses=10.10.4.1"

corp5.com Password = "cisco", Service-Type = Outbound-User
      cisco-avpair = "vpdn:tunnel-id=NAS",
      cisco-avpair = "vpdn:nas-password=corp5secret",
      cisco-avpair = "vpdn:gw-password=corp5secret",
      cisco-avpair = "vpdn:ip-addresses=10.10.5.1"

corp6.com Password = "cisco", Service-Type = Outbound-User
      cisco-avpair = "vpdn:tunnel-id=NAS",
      cisco-avpair = "vpdn:nas-password=corp6secret",
      cisco-avpair = "vpdn:gw-password=corp6secret",
      cisco-avpair = "vpdn:ip-addresses=10.10.6.1"

corp7.com Password = "cisco", Service-Type = Outbound-User
      cisco-avpair = "vpdn:tunnel-id=NAS",
      cisco-avpair = "vpdn:nas-password=corp7secret",
      cisco-avpair = "vpdn:gw-password=corp7secret",
      cisco-avpair = "vpdn:ip-addresses=10.10.7.1"

corp8.com Password = "cisco", Service-Type = Outbound-User
      cisco-avpair = "vpdn:tunnel-id=NAS",
      cisco-avpair = "vpdn:nas-password=corp8secret",
      cisco-avpair = "vpdn:gw-password=corp8secret",
      cisco-avpair = "vpdn:ip-addresses=10.10.8.1"

corp9.com Password = "cisco", Service-Type = Outbound-User
      cisco-avpair = "vpdn:tunnel-id=NAS",
      cisco-avpair = "vpdn:nas-password=corp9secret",
      cisco-avpair = "vpdn:gw-password=corp9secret",
      cisco-avpair = "vpdn:ip-addresses=10.10.9.1"

corp10.com Password = "cisco", Service-Type = Outbound-User
      cisco-avpair = "vpdn:tunnel-id=NAS",
      cisco-avpair = "vpdn:nas-password=corp10secret",
      cisco-avpair = "vpdn:gw-password=corp10secret",
      cisco-avpair = "vpdn:ip-addresses=10.10.10.1"

```

The following configuration could run on a Cisco 4500 series home gateway router that is used in a large-scale VPDN solution:

```

!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname CORP1_HomeGateway
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
!
username NAS password corplsecret
username NAS password corplsecret
username pcuser@corp1.com password cisco

```

## Remote PCs Dialing In to a Virtual Private Dial Network

---

```
vpdn enable
vpdn incoming ISP corp1.com virtual-template 1
!
interface Ethernet0
 ip address 4.1.1.1 255.255.255.0
!
interface Ethernet1
 no ip address
 shutdown
!
interface Serial0
 ip address 10.10.1.1 255.255.255.252
 encapsulation ppp
!
interface Serial1
 no ip address
 shutdown
!
interface Serial2
 no ip address
 shutdown
!
interface Serial3
 no ip address
 shutdown
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 peer default ip address pool corp1_pool
 ppp authentication chap pap
!
router eigrp 2
 network 2.0.0.0
 no auto-summary
!
ip local pool corp1_pool 4.1.1.3 4.1.1.52
ip classless
!
!
line con 0
line aux 0
line vty 0 4
```