



Telco and ISP Dial Scenarios and Configurations

This chapter provides sample hardware and software configurations for specific dial scenarios used by telcos, Internet service providers (ISPs), regional Bell operating companies (RBOCs), inter-exchange carriers (IXCs), and other service providers. Each configuration in this chapter is designed to enable IP network traffic with basic security authentication.

The following scenarios are described:

- Scenario 1—[Small- to Medium-Scale POPs](#)
- Scenario 2—[Large-Scale POPs](#)
- Scenario 3—[PPP Calls over X.25 Networks](#)



Note

In all of these scenarios, you can replace the Cisco AS5200 access server with Cisco AS5300 or Cisco AS5800 access server. This hardware exchange provides higher call density performance and increases the number of PRI interfaces and modem ports on each chassis.

Small- to Medium-Scale POPs

Many small-to-medium-sized 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 LANs. Using the Windows 95 dialup software, remote clients initiate analog or digital connections using modems or home office ISDN BRI terminal adapters.

This section provides three types of single user dial-in scenarios for service providers:

- [Individual Remote PCs Using Analog Modems](#)
- [Individual PCs Using ISDN Terminal Adapters](#)
- [Mixture of ISDN and Analog Modem Calls](#)



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.



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

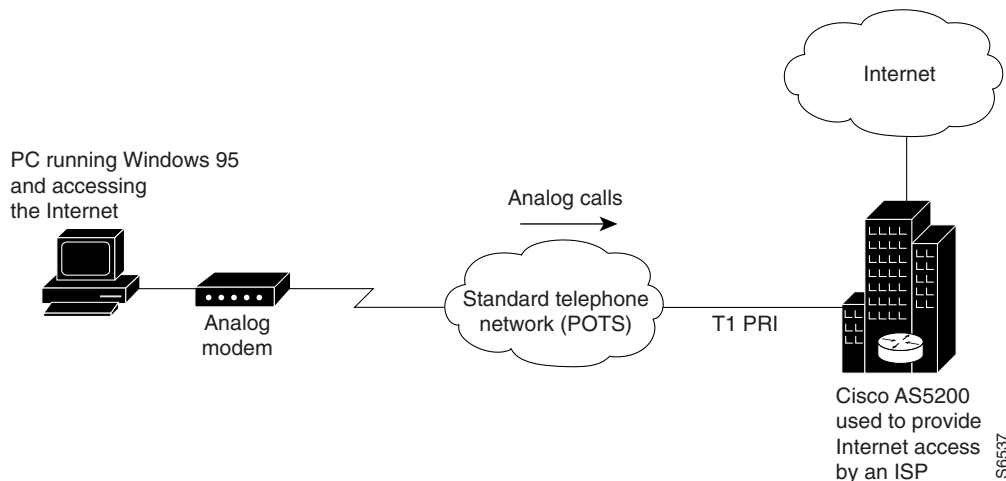
Individual Remote PCs Using Analog Modems

ISPs can configure a single Cisco access server to receive analog calls from remote PCs connected to modems, as shown in [Figure 1](#). The point of presence (POP) at the ISP central site could also be a Cisco 2511 access server connected to external modems.

Network Topology

[Figure 1](#) shows a small-scale dial-in scenario using modems.

Figure 1 Remote PC Using an Analog Modem to Dial In to a Cisco Access Server



Running Configuration for ISDN PRI

The following sample configuration runs on the Cisco access server, as shown in [Figure 1](#), which enables remote analog users to dial in:

```

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
    !
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 the configuration file of a remote security server:

```

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"
    }
}

```

Running Configuration for Robbed-Bit Signaling

The following example shows a single Cisco access server configured to support remote client PCs dialing in with analog modems over traditional 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).

```

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
 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

```

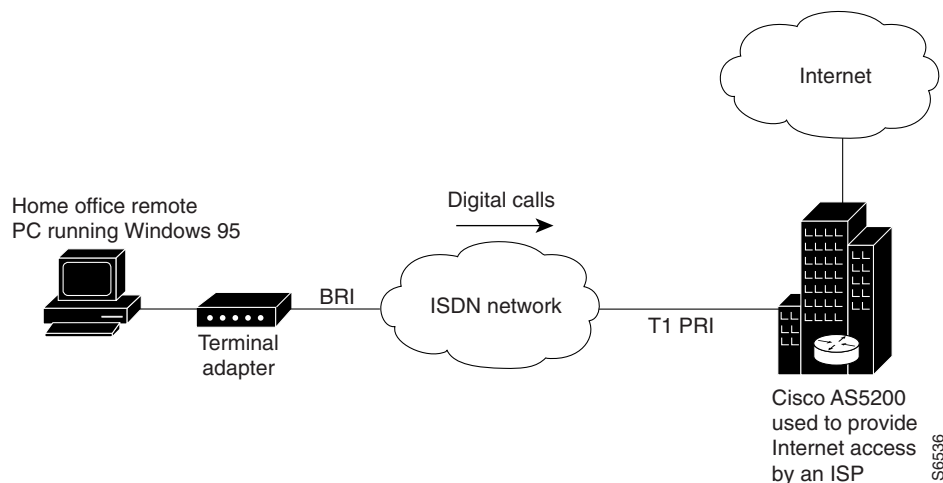
Individual PCs Using ISDN Terminal Adapters

ISPs can configure a single Cisco access server to receive digital multilink calls from remote PCs connected to terminal adapters, as shown in [Figure 2](#). The POP at the central site of the ISP can be any Cisco router that supports ISDN PRI, such as the Cisco 4700-M router loaded with a channelized T1 PRI network module.

Network Topology

[Figure 2](#) shows a small-scale dial-in scenario using terminal adapters.

Figure 2 Remote PC Using a Terminal Adapter to Dial In to a Cisco Access Server



To configure one Cisco access server to accept both incoming ISDN and analog calls from individual terminal adapters and modems, see the section “[Mixture of ISDN and Analog Modem Calls](#)” later in this chapter.

Terminal Adapter Configuration Example

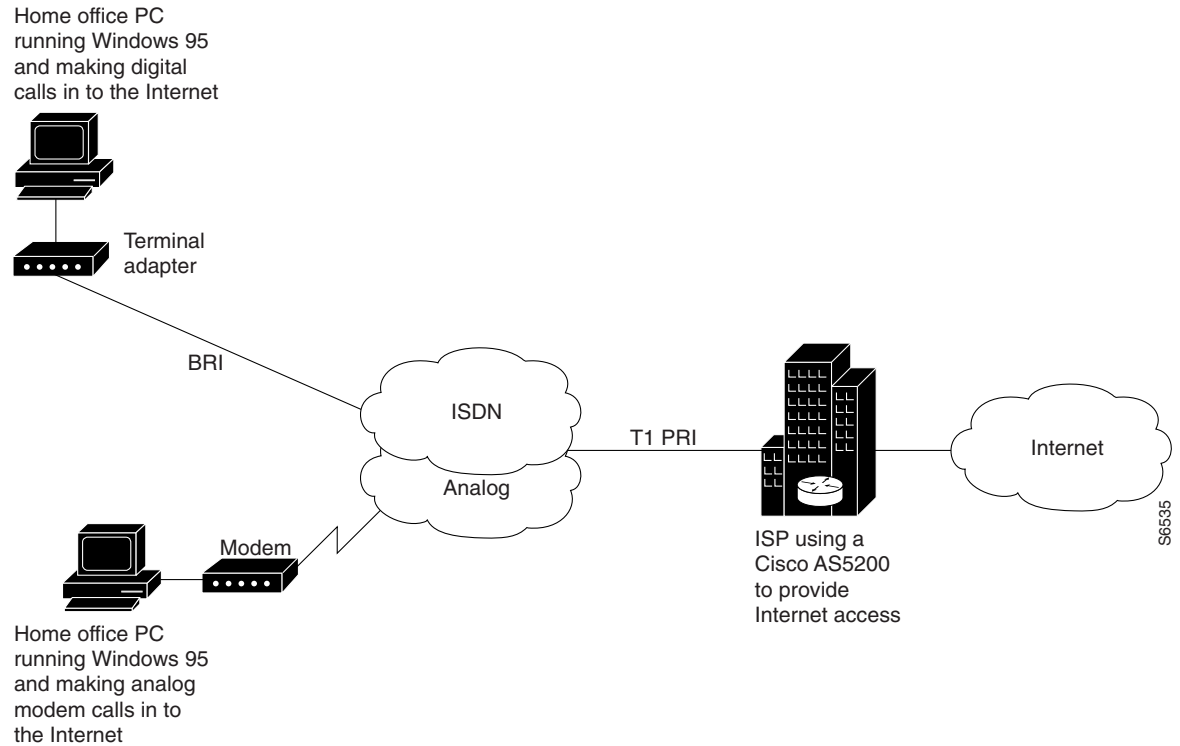
The following example configures a Cisco access server to enable PCs fitted with internal or external terminal adapters to dial in to an IP network. The terminal adapter configuration is set up for asynchronous-to-synchronous PPP conversion. In some cases, PPP authentication must be set up for the Password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

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

Mixture of ISDN and Analog Modem Calls

ISPs can configure a single Cisco access server to receive calls from a mixture of remote PCs connected to terminal adapters and modems, as shown in [Figure 3](#).

Figure 3 Remote PCs Making Digital Calls and Analog Calls to a Cisco Access Server

Combination of Modem and ISDN Dial-In Configuration Example

The following example shows a combination of the modem and ISDN dial-in configurations. Using the bearer capability information element in the call setup packet, the incoming calls are labeled as data or voice. After the calls enter the access server, they are 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, see the chapter “Enterprise Dial Scenarios and Configurations” in this publication.

```

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
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
```

Large-Scale POPs

This section describes how to set up a stack of access servers for a large-scale dial solution and includes the following sections:

- [Scaling Considerations](#)
- [How Stacking Works](#)
- [Stack Group of Access Servers Using MMP with an Offload Processor Examples](#)

Scaling Considerations

Because of the significant increase in demand for Internet access, large POPs are required by many Telcos and ISPs. Internet access configurations can be set up to enable users who dial in with individual computers to make mixed ISDN multilink or modem connections using a stack of Cisco access servers that run Multichassis Multilink PPP (MMP).

You must consider scalability and call density issues when designing a large-scale dial-in POP. 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 percent modem calls, 10 to 25 percent ISDN calls (terminal adapters or routers), and support for fewer than 96 (T1) to 116 (E1) simultaneous dial-in connections.	Two Cisco access servers configured for IP, basic security, MMP, L2F, and no offload server. Note Effective with Cisco Release 12.4(11)T, the L2F protocol was removed in Cisco IOS software.
PCs dialing in, less than 50 percent modem calls, more than 50 percent ISDN calls (terminal adapters or routers), dial-in only, and 250 or more simultaneous links into the offload server.	Three or more Cisco access servers configured for IP, remote security, MMP, and L2F. Each Cisco access server is configured to offload its segmentation and reassembly of the multilink sessions onto an offload server, such as a Cisco 7202 or Cisco 4700 router. Note Effective with Cisco Release 12.4(11)T, the L2F protocol was removed in Cisco IOS software.

**Note**

Depending on the size of your POP requirement, you can replace the Cisco AS5200 access server with a Cisco AS5300, Cisco AS5800, or Cisco AccessPath. This hardware exchange provides higher call density performance and increases the number of ISDN PRI ports, channelized ports, and modem ports on each chassis.

How Stacking Works

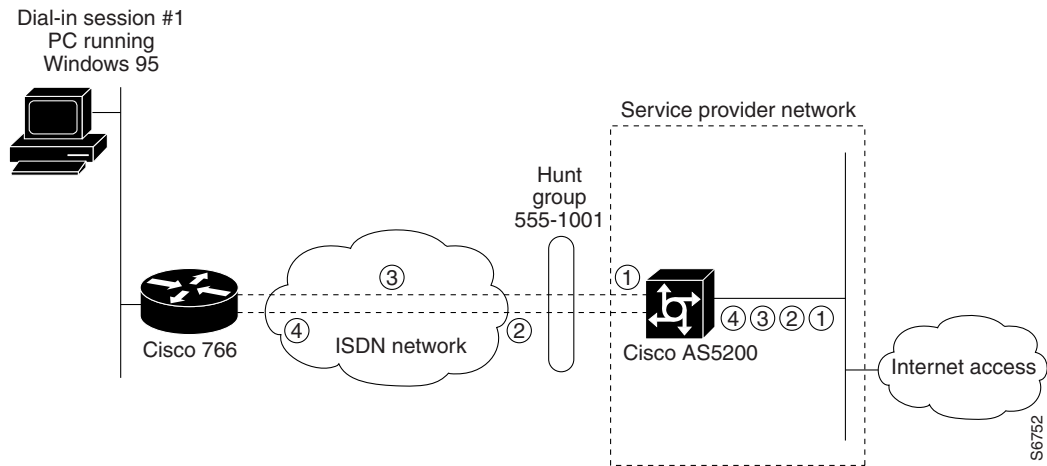
Before you install and configure a stack of access servers, you should understand the basic concepts described in the following sections and how they work together in a large-scale dial-in solution:

- [A Typical Multilink PPP Session](#)
- [Using Multichassis Multilink PPP](#)
- [Setting Up an Offload Server](#)
- [Using the Stack Group Bidding Protocol](#)
- [Using L2F](#)

A Typical Multilink PPP Session

A basic multilink session is an ISDN connection between two routing devices, such as a Cisco 766 router and a Cisco AS5200 access server. [Figure 4](#) 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 (MLP) session is brought up. The Cisco 766 router sends four packets across the network to the Cisco AS5200, which in turn reassembles the packets back into the correct order and sends them out the LAN port to the Internet.

Figure 4 A Typical Multilink PPP Session



Using Multichassis Multilink PPP



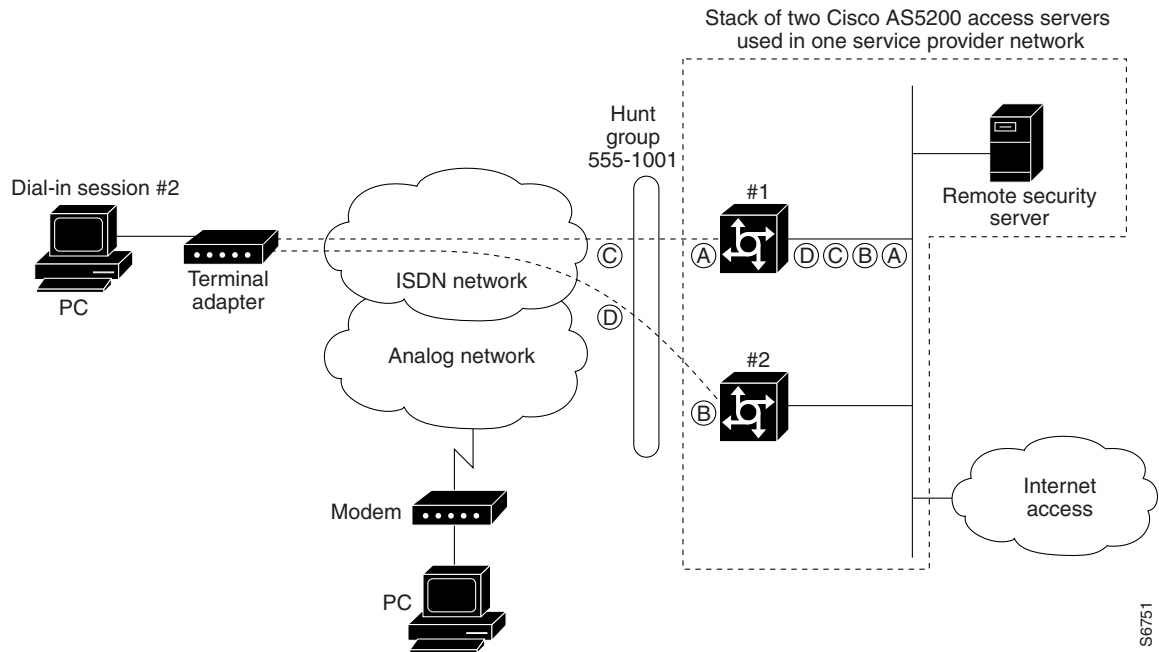
Note

Effective with Cisco Release 12.4(11)T, the **L2F protocol** was removed in Cisco IOS software.

The dial solution becomes more complex when the scenario is scaled to include multiple multilink calls connecting across multiple chassis. [Figure 5](#) shows a terminal adapter making a call in to the Cisco AS5200, labeled #1. However, only one of the access server's 48 B channels is available to accept the call. The other channels are busy with calls. As a result, 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 bundle master. The bundle master takes ownership of the MLP session with the remote device. The Multichassis Multilink PPP (MMP) protocol forwards the second link from device #2 to the bundle master, 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.

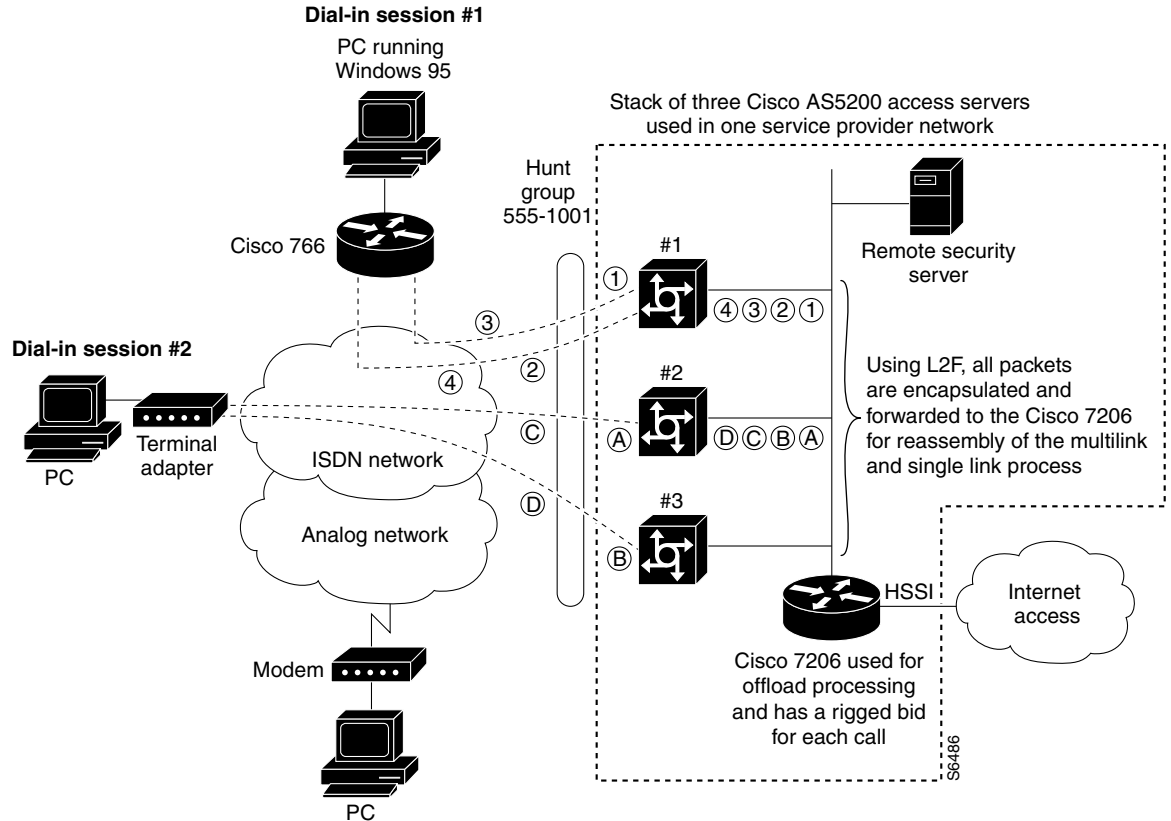
Figure 5 A Stack Group of Access Servers Using MMP Without an Offload Processor



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 access servers to a router with a more powerful CPU, such as the Cisco 4700-M or Cisco 7206. We recommend that you include an offload server for dial-in solutions that support more than 50 percent ISDN calls or more than 10 multilink sessions per Cisco access server. (See [Figure 6](#).)

Figure 6 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. SGBP unites each Cisco access server 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 devices' CPU should be in charge of running the multilink session and packet reassembly—the duty of the bundle master. The goal of SGBP is to find a common place to forward the links and ensure that this destination has enough CPU power to perform the segmentation and packet reassembly. (See [Figure 6](#).)

When SGBP is configured on each Cisco access server, 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:

- 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.
- If I do not have an existing call for walt@options.com, then bid a value that is proportional to how much CPU power I have available.
- How busy am I supporting other users?



Note

An offload server will always serve as the bundle master by bidding a higher value than the other devices.

Using L2F



Note

Effective with Cisco Release 12.4(11)T, the **L2F protocol** was removed in Cisco IOS software.

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 bundle master 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. (Refer to [Figure 6](#).)

Stack Group of Access Servers Using MMP with an Offload Processor Examples

The following sections provide examples for the devices shown in [Figure 6](#):

- [Cisco Access Server #1](#)
- [Cisco Access Server #2](#)
- [Cisco Access Server #3](#)
- [Cisco 7206 as Offload Server](#)
- [RADIUS Remote Security Examples](#)



Note

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

Cisco Access Server #1

The following configuration runs on the Cisco access server labeled #1 in [Figure 6](#):

```

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 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
!
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 Access Server #2

The following configuration runs on the Cisco access server labeled #2 shown in [Figure 6](#):

```

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 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
 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 Access Server #3

The following configuration runs on the Cisco access server labeled #3 in [Figure 6](#):

```

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 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
!
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 as Offload Server

The following configuration runs on the Cisco 7206 router shown in [Figure 6](#):



Note

Any Cisco router that has a powerful 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 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 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-Templat1
 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-Templatel
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 RADIUS examples in the following sections use the Internet Engineering Task Force (IETF) syntax for the attributes:

- [User Setup for PPP](#)
- [User Setup for PPP and Static IP Address](#)
- [Enabling Router Dial-In](#)
- [User Setup for SLIP](#)
- [User Setup for SLIP and Static IP Address](#)
- [Using Telnet to connect to a UNIX Host](#)
- [Automatic rlogin to UNIX Host](#)

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.

User Setup for PPP

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 Dynamic Host Configuration Protocol (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

```

User Setup for PPP and Static IP Address

The following example shows a user setup for PPP and a static IP address that stays with the user across all connections. Make sure that 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 = 10.1.1.1

```

Enabling Router Dial-In

The following 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.

```

routeme Password = "cisco"
CHAP-Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
Framed-IP-Address = 10.1.1.1
Framed-Route = "10.2.1.0/24 10.1.1.2"

```

User Setup for SLIP

The following example shows a user setup for SLIP. 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

```

User Setup for SLIP and Static IP Address

The following example shows a user setup for SLIP and a static IP address that stays with the user across all connections. Make sure that 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 = 10.1.1.13

```

Using Telnet to connect to a UNIX Host

The following example automatically uses Telnet to connect 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 = 10.2.1.1
```

Automatic rlogin to UNIX Host

The following example automatically uses rlogin to connect the user to a UNIX host:

```
rloginme Password = "cisco"
      Service-Type = Login,
      Login-Service = Rlogin,
      Login-IP-Host = 10.3.1.2
```

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**

PPP Calls over X.25 Networks

Remote PCs stationed in X.25 packet assembler-disassembler (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 that 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 use installed bases of X.25 equipment and cost less to operate than connecting over the standard telephone network.



Note

This dial-in scenario can also be used as an enterprise solution. 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.

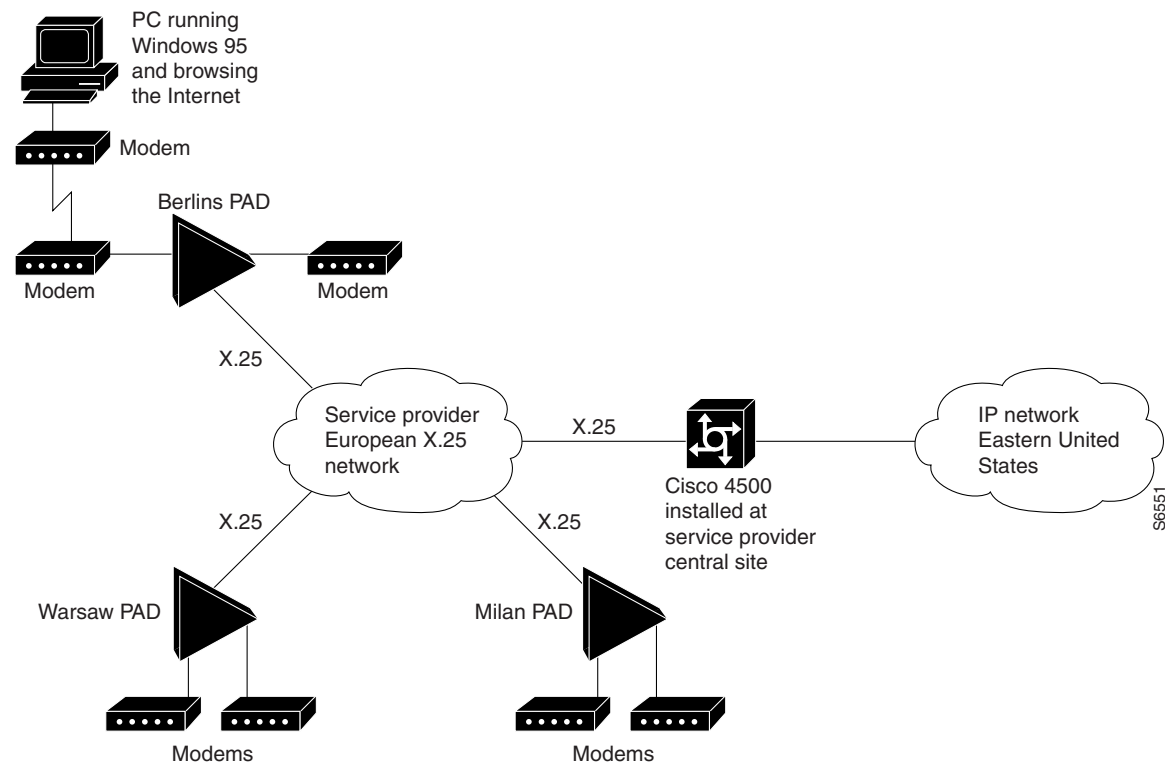
Overview

Many cities throughout the world have large installed bases of PCs that interface 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 that have large investments in X.25 networks are upgrading their outdated equipment and creating separate networks for PPP connections. Because this upgrade process takes substantial 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.

Remote PC Browsing Network Topology

Figure 7 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 that is heavily invested in X.25 equipment, that is currently upgrading its outdated equipment, and that is creating separate networks for PPP connections. In this topology, the Cisco 4500 router 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.

Figure 7 Remote PC Browsing the Internet Through an X.25 PAD Call and a Cisco 4500 Router



For more information about configuring protocol translation, see the chapter “Configuring Protocol Translation and Virtual Asynchronous Devices” in the *Cisco IOS Terminal Services Configuration Guide*.

Protocol Translation Configuration Example

In the following example, PAD callers that dial 4085551234 receive a router prompt. PAD callers that dial 4085555123401 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 4500 router. Additionally, a loopback interface network can be created and the X.25 addresses can be set. However, a routing protocol must be run to advertise the loopback interface network if this method is used.



Note

Be sure to include your own IP addresses, host names, and security passwords where appropriate in the following examples.

```

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

x25 route 11111 interface Dialer0
x25 route 44444 interface Dialer0
!

```

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2001–2009 Cisco Systems, Inc. All rights reserved.

