This case study describes the design of an access network that allows a large number of remote sites to communicate with an existing central-site network. The remote sites consist of local-area networks (LANs) that support several workstations. The workstations run transaction processing software that accesses a database located at the central site. The following objectives guided the design of the access portion of the network:

- The existing network could not be modified to accommodate access by the remote sites.
- The central site must be able to connect to any remote site at any time, and any remote site must be able to connect to the central site at any time.
- When choosing between alternative technologies, choose the most cost-effective technology.
- The design must be flexible enough to accommodate additional remote sites in the future.

Contents

Network Design Considerations

The following considerations influenced the design of this network:

- Traffic Patterns
- Media Selection
- Application Protocol Requirements

Traffic Patterns

An analysis of the anticipated traffic indicated that each remote site would call the central site an average of four times an hour throughout the business day. This type of traffic pattern means that cost savings can be realized at the central site by providing one telephone line for every 2.5 remote sites (for a total of 48 telephone lines). To spread the calls evenly among the 48 lines, the remote sites connect through a hunt group. The hunt group provides an additional benefit in that all of the remote routers dial the same telephone number to access the central site, which makes the configurations of the remote site routers easier to maintain.

In order to complete a transaction initiated by a remote-site, the central site sometimes needs to call that remote site shortly after it has disconnected from the central site. To make this possible, the access network must converge rapidly. The central site also calls the remote sites periodically to update the transaction processing software on the remote workstations.

Media Selection

The designers chose asynchronous dial-up technology through the Public Switched Telephone Network (PSTN) for the following reasons:

- Availability-PSTN is available at all of the remote sites. Potential alternatives, such as Frame Relay and Integrated Digital Services Network (ISDN), were not available at some of the remote sites.
- Bandwidth-The transaction processing software causes a small amount of data to be transferred between the remote sites and the central site. For this type of low-bandwidth application, the bandwidth provided by asynchronous dial-up is acceptable. Occasionally, the central site dials the remote sites in order to maintain the transaction processing software on the remote clients. This activity will occur at night (in the absence of transaction processing activity), so the bandwidth provided by asynchronous dial-up is adequate.

- Cost-Given the low-bandwidth requirement, the cost of installing and operating Frame Relay or ISDN equipment could not be justified.

Note: Although the network described in this case study uses asynchronous dial-up technology over the PSTN, most of the concepts, such as routing strategy and addressing, also apply when scaling other circuit-switched technologies (such as ISDN).

Application Protocol Requirements

The remote workstations run transaction processing software that uses the Transmission Control Protocol /Internet Protocol (TCP/IP) to connect to a database located at the central site. The remote workstations have no need to run any other network-layer protocol. Given this requirement, the most cost-effective choice of router for the remote site is a router that provides an Ethernet interface and an asynchronous interface, and that supports the Routing Information Protocol (RIP).

The Hardware Solution

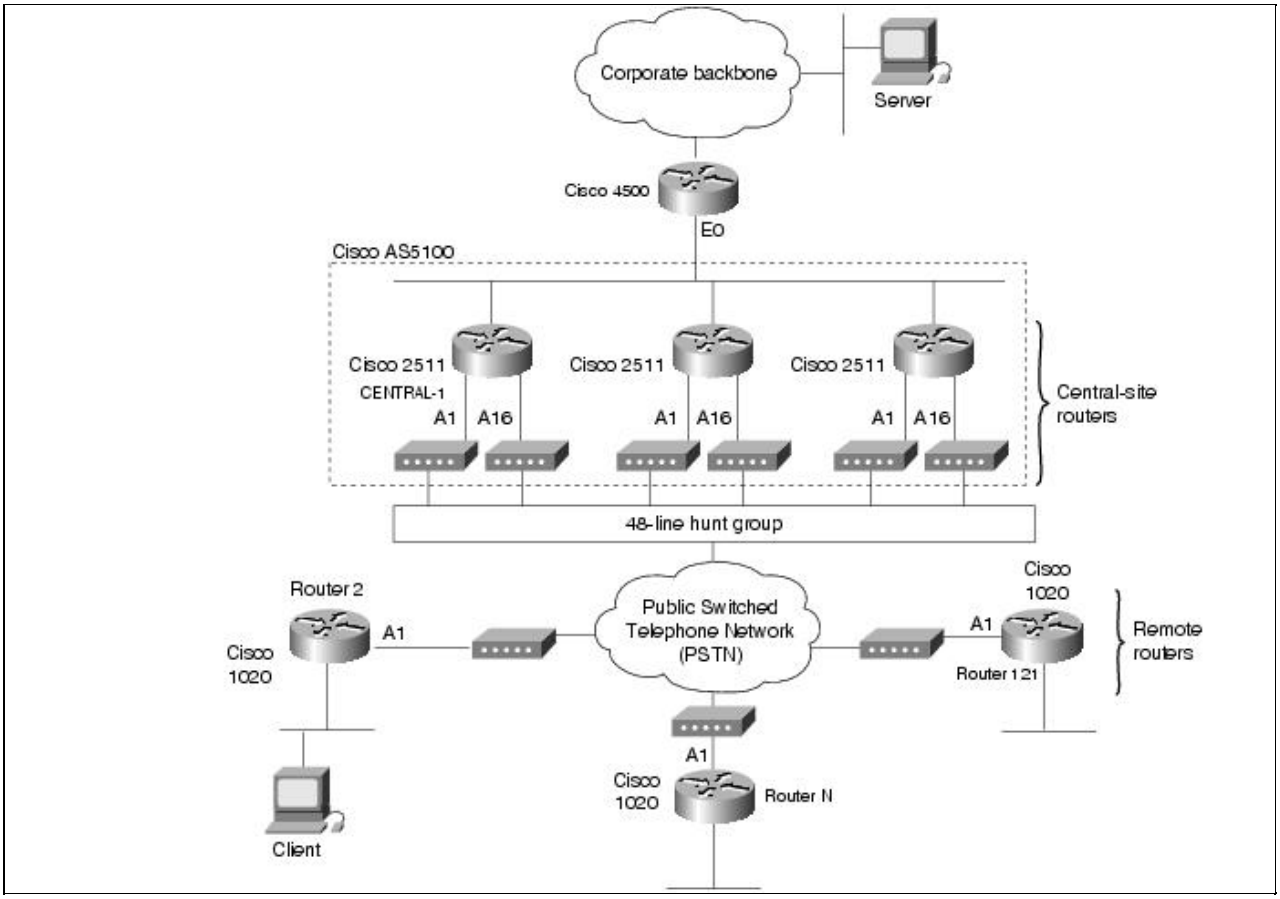
A Cisco AS5100 is installed at the central site to provide 48 asynchronous interfaces. The Cisco AS5100 consists of three access server cards based on the Cisco 2511 access server, making the Cisco AS5100 equivalent to three Cisco 2511 access servers. Each access server card provides 16 asynchronous lines. Each asynchronous line is equipped with a built-in U.S. Robotics Courier modem.

Note: For the purposes of this case study, the three Cisco AS5100 access server cards are referred to as the central-site access routers.

Each remote site is equipped with a Cisco 1020 router. The Cisco 1020 provides a single asynchronous interface and an Ethernet interface for connecting to the remote site LAN. The Cisco 1020 runs a limited set of protocols, including TCP/IP and RIP. U.S. Robotics Sportster modems provide connectivity at the remote sites. Using the same brand of modem throughout the access network simplifies chat scripts and modem definition, and makes the network more manageable.

A Cisco 4500 controls routing between the new access portion of the network and the backbone. In particular, the Cisco 4500 ensures that when hosts on the other side of the backbone need to connect to a remote site, the connection is made through the optimum central-site access router. Figure: Remote access topology shows the topology of the access portion of the network.

Figure: Remote access topology



The Software Solution

The configuration of the central-site access routers and the remote site routers must provide the following:

- Authentication
- Network Layer Addressing
- Routing Strategy

Authentication

Traffic between the remote sites and the central site includes confidential information. For that reason, authentication is a primary concern. There are two ways for sites to authenticate themselves:

- Point-to-Point Protocol (PPP) authentication-Either the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP) can be used.
- Login authentication-With login authentication, the router prompts for a host name and password when a remote router dials in. The remote router logs in and starts PPP.

In either case, the database of usernames and passwords can be stored locally or on an extended Terminal Access Controller Access System (TACACS+) server. TACACS+ provides centralized password management for all the central-site access routers and detailed accounting information about connections to and from the remote sites.

For the purposes of this network design, login authentication is used because it allows the remote sites to announce their IP addresses to the central-site access routers, as described in the section "Network Layer Addressing" later in this article. Alternatively, PPP could be started automatically if TACACS+ were used to

Figure: Remote access topology

support per-user IP address assignment.

Network Layer Addressing

Network layer addressing is accomplished through two strategies:

- Subnet Address Assignment
- Next Hop Address

Subnet Address Assignment

The remote routers and the central-site access routers have no need to connect to the Internet, so they use RFC 1597 addresses. The Class B address 172.16.0.0 is used for the entire access portion of the network, and Class C equivalent addresses are assigned to the remote routers. Each subnet gets one Class C equivalent (172.16.x.0 with a mask of 255.255.255.0), which makes addressing easy to manage. Network 172.16.1.0 is reserved for numbering the dialer cloud later if needed. (The dialer cloud is defined as the subnet to which all of the asynchronous interfaces are attached.)

Initially, the dialer cloud is unnumbered. If, in the future, the dialer cloud were to be numbered, the following questions must be considered:

- Can the dialer cloud use the same subnet mask as the remote sites? If not, variable length subnet mask (VLSM) support will be required. (RIP does not support VLSM.)
- Would the use of multiple subnetted Class C addresses cause discontiguous subnets at the remote sites? If so, discontiguous subnet support will be required. (RIP does not support discontiguous subnets.)

In this network, these issues are not a problem. A mask of 255.255.255.0 can be used everywhere, so there are no VLSM concerns. All subnets are from the same major Class B network, so there are no discontiguous subnet concerns. Table: Addressing Summary summarizes the addressing for the access portion of the network.

Table: Addressing Summary

Site	Subnet	Mask
Central access site	172.16.1.0	255.255.255.0
Router2	172.16.2.0	255.255.255.0
Router3	172.16.3.0	255.255.255.0
...	...	...
Router121	172.16.121.0	255.255.255.0

Next Hop Address

To facilitate an accurate routing table and successful IP Control Protocol (IPCP) address negotiation, all next-hop IP addressing must be accurate at all times. To accomplish this, the remote sites need to know the IP address that they will dial in to, and the central site needs to know the IP address of the remote site that has dialed in.

All central-site access routers use the same IP address on all of their asynchronous interfaces. This is accomplished by configuring the Dialer20 interface for IP unnumbered off of a loopback interface. The IP address of the loopback interface is the same on all of the central-site access routers. This way, the remote routers can be configured with the IP address of the router to which it connects, regardless of which router the remote router dials in to.

The remote router needs to announce its IP address to the central-site router when the remote router connects. This is accomplished by having the remote router start PPP on the central site using the EXEC command **ppp 172.16.x.1**. To support this, each central-site access router is configured with the **async dynamic address** interface configuration command.

Note: The autoselect feature allows the router to start an appropriate process, such as PPP, automatically when it receives a starting character from the router that has logged in. To use autoselect, a mechanism for supporting dynamic IP address assignment would be required, such as per-user address support in TACACS+.

Routing Strategy

The development of the routing strategy for this network is based on the following two requirements:

- When a particular remote site is not dialed in to the central site, that remote site must be reachable through any central-site access router by means of a static route configured in each central-site access router.
- When a particular remote site router is logged in to a central-site access router, that remote site must be reachable through that central-site access router by means of the dynamic route that has been established for that connection and propagated to the backbone.

To meet these requirements, the central-site access routes advertise the major network route of the remote sites to the Cisco 4500. All routes to the remote sites are equal-cost through all of the central-site access routers. Each central-site access router is configured to have a static route to each remote site. To allow the Cisco 4500 to use all of the central-site access routers for connecting to the remote sites, the **no ip route-cache** interface configuration command is configured on Ethernet interface 0 of the Cisco 4500, disabling fast switching of IP to the subnet shared with the central-site access routers. This causes the Cisco 4500 to alternate between the three access routers when initiating outbound calls. This strategy increases network reliability for those cases when one of the access routers goes down.

When a remote router logs in, it announces its IP address and sends a RIP flash. The RIP flash causes a dynamic route to the remote site to be installed immediately in the routing table of the central-site access router. The dynamic route overrides the static route for the duration of the connection.

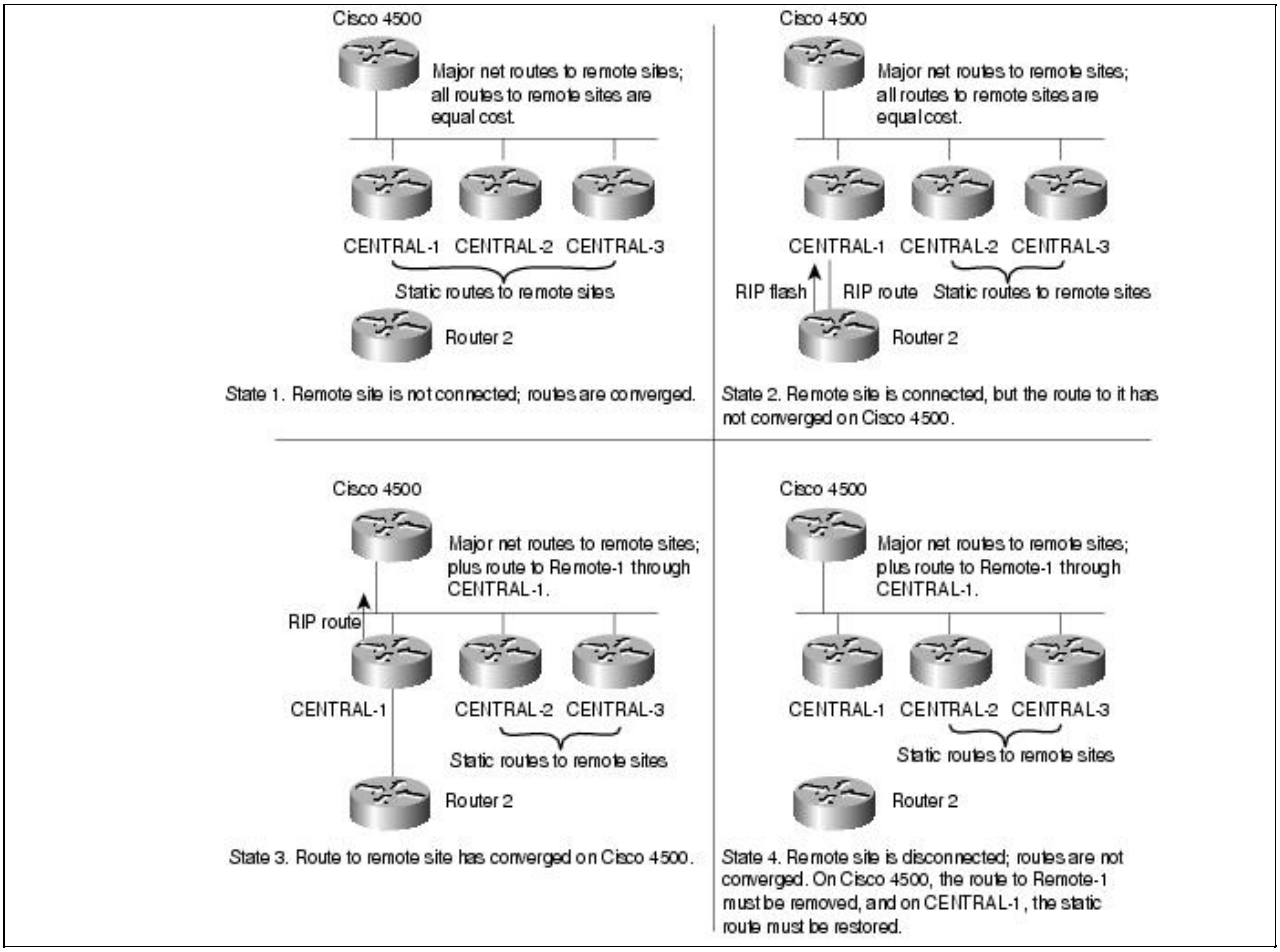
Next, the central-site access router redistributes the RIP route into Open Shortest Path First (OSPF) and sends the route to all of its OSPF neighbors, including the Cisco 4500, which installs it in its routing table. The Cisco 4500 now has a major network route to all of the remote sites, plus a dynamic route to the specific remote site that has logged in. If a central-site host needs to communicate with a particular remote site that is currently logged in, it does so through the dynamic route.

When the remote site logs out, the dynamic route must be removed from the Cisco 4500, and the static route to the remote site must be restored on the central-site access router into which the remote router logged in.

If a central-site host requires communication with a remote site that is not logged in, it will use the major network route defined in the Cisco 4500. A central-site access router, selected in round-robin fashion, is used to initiate the call to the remote site via the static route that is defined for it in the configuration for the selected access router. As in the case of a remote site that calls the central site, once the connection is made, the remote-site router sends a RIP flash that causes a dynamic route to the remote site to be installed immediately in the routing table of the central-site access router. This dynamic route is redistributed into OSPF and is installed in the routing table of the Cisco 4500. Figure: Routing strategy state diagram uses a

state diagram to summarize the routing strategy.

Figure: Routing strategy state diagram



The following convergence issues pertain to the state diagram shown in Figure: Routing strategy state diagram:

- During the time between State 2 and State 3, a host at the central site might initiate a call to the remote site. Until State 3, at which time the routes converge on the Cisco 4500, any central-site access router that dials the remote site will fail with a busy signal. In practice, only one call fails: by the time a second connection attempt is made, the routes will have converged in State 3, the dynamic route will be available for use, and there will be no need to make another call.
- When the remote site disconnects, at minimum 120 seconds will elapse before the static route is restored to the routing table of the central-site access router on which the remote site logged in. First, up to 35 seconds might elapse before RIP determines that the remote site has disconnected and is no longer sending RIP updates. Sixty seconds later, the central-site access router scans its routing table and restores one of the two static routes for the remote site, and sixty seconds after that, it scans its routing table again and restores the second of the two static routes. (For information about why there are two static routes for each remote site, see the section "Static Routing Configuration" later in this article.)

Note: Fast install of static routes is a new feature in Cisco IOS Software Release 11.1 that quickly

converges back to the static route when a remote site disconnects.

If, before convergence occurs, the Cisco 4500 directs a call through CENTRAL-1 to Router 2, the call will fail and must be retried. IP fast switching is turned off on the Cisco 4500, so the Cisco 4500 (which is using equal-cost paths to each of the central-site access routers) will send the next packet through CENTRAL-2 or CENTRAL-3 (which still have a static route for Router 2) and the call will go through.

Note: When developing the routing strategy for this network, the designers considered the use of snapshot routing, which reduces connection cost by limiting the exchange of routing protocol updates. For snapshot routing to work, each remote site must connect to the same access router every time it dials into the central site. In this design, the remote routers connect to the central-site access routers through a hunt group, so there is no way to control to which central-site access router a remote router will connect for any particular connection. Therefore, snapshot routing cannot be used for this design.

Configuring the Central Site Access Routers

This section describes how the configuration of the central-site access routers implements authentication, network layer addressing, and the routing strategy. The configuration for each central-site access router is the same with the following exceptions:

- The IP address specified for loopback interface 0
- The IP address specified for Ethernet interface 0
- The name of the router as specified by the **hostname** global configuration command

This discussion is divided among the following topics:

For the complete configuration see the section "CENTRAL-1 Configuration" later in this article.

Username Configuration for the Remote Sites

The configuration of each central-site access router includes the following **username** global configuration commands:

```
username Router2 password 7 071C2D4359
...
username Router121 password 7 0448070918
```

Each remote router can dial in to any of the three central-site access routers, so there is a **username** global configuration command for each remote router. When a remote router logs in, it specifies a name (for example, Router2) and a password (for example, outthere) that must match the values specified by a

Figure: Routing strategy state diagram

username command. Each remote site uses a chat script to log in and specify its host name (which must match a value specified by the **username** command) and password. (For information about the chat script that the remote sites use, see the section Chat Script Configuration for Dialing the Central Site later in this article.)

Dial-Up Configuration for the Remote Sites

The configuration of each central-site access router includes the following **chat-script** global configuration commands:

```
chat-script CALL1020 ABORT ERROR ABORT BUSY TIMEOUT 30 "" "ATDT\T" "CONNECT" \c
chat-script REM TIMEOUT 40 "name:" "CENTRAL" "word:" "secret"
chat-script usrv32bis "" "AT&F1S0=1&d2" "OK" ""
!
interface dialer 20
dialer map ip 172.16.2.1 name Router2 modem-script CALL1020 system-script REM 5551234
...
dialer map ip 172.16.121.1 name Router2 modem-script CALL1020 system-script REM 5555678
!
line 1 16
script reset usrv32bis
```

The three **chat-script** global configuration commands establish three scripts named CALL1020, REM, and usrv32bis. CALL1020 and REM are invoked by the **dialer map** commands to dial and log in to the remote sites, respectively. The **script reset** command specifies that the USRV32BIS script is to be run whenever an asynchronous line is reset in order to ensure that the central-site modems are always configured correctly.

Loopback Interface Configuration

The configuration of each central-site access router includes the commands for configuring loopback interfaces. The IP address for loopback interface 0 is unique for each access router and, to satisfy the rules by which OSPF selects the router ID, must be the highest loopback IP address on the router. The IP address for loopback interface 1 is the same for each central-site access router. The commands are as follows:

```
interface loopback 0
ip address 172.16.254.3 255.255.255.255
...
interface loopback 1
ip address 172.16.1.1 255.255.255.0
```

The goal is for all three access routers to appear to have the same IP address during IPCP negotiation with the remote sites. (IPCP is the part of PPP that brings up and configures IP support.) This goal is accomplished by creating a loopback interface, assigning to it the same IP address on each central-site access router, and running the **ip unnumbered** interface configuration command using the loopback interface address. The problem with this strategy is that OSPF takes its router ID from the IP address of a loopback interface, if one is configured, which would mean that all three access routers would have the same OSPF router ID.

The solution is to create loopback interface 0 and assign to it a unique IP address (which results in a unique OSPF router ID for each router). The configuration then creates loopback interface 1 and assigns to it the same IP address on each router. Loopback interface 1 allows the **ip unnumbered** command to be applied to dialer rotary group 20 later in the configuration.

Asynchronous Line Configuration

The configuration of each central-site access router includes the following commands for configuring each asynchronous interface:

```
interface async 1
ip unnumbered loopback 1
async dynamic address
async dynamic routing
async mode interactive
dialer in-band
dialer rotary-group 20
```

For each of the 16 asynchronous interfaces provided by the access router, the configuration uses the **ip unnumbered** interface configuration command to specify that the asynchronous interface is to use the IP address of loopback interface 1 as the source address for any IP packets that the asynchronous interface generates. The IP address of loopback interface 1 is also used to determine which routing processes are sending updates over the asynchronous interface.

The **async dynamic address** interface configuration command enables dynamic addressing on the asynchronous interface. This command is required to allow each remote router to specify its IP address when it logs in. The **async dynamic routing** interface configuration command allows the interface to run a routing protocol, in this case RIP.

The **async mode interactive** interface configuration command allows a remote router to dial in and access the EXEC command interface, which allows the remote router to start PPP and specify its IP address.

The **dialer in-band** interface configuration command allows chat scripts to be used on the asynchronous interface. The chat scripts allow the access router to dial the remote sites. The **dialer rotary-group** interface configuration command assigns each asynchronous interface to dialer rotary group 20.

Dialer Interface Configuration

The configuration of each central-site access router includes the following commands for configuring dialer rotary group 20:

```
interface dialer 20
ip unnumbered loopback 1
encapsulation ppp
dialer in-band
dialer idle-timeout 60
dialer map ip 172.16.2.1 name Router2 modem-script CALL1020 system-script REM 5551234
...
dialer map ip 172.16.121.1 name Router121 modem-script CALL1020 system-script REM 5555678
dialer-group 3
dialer-list 3 list 101
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 520
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

The **interface dialer** global configuration command defines dialer rotary group 20. Any interface configuration commands that are applied to a dialer rotary group apply to the physical interfaces that are its members. When the router's configuration includes multiple destinations, any of the interfaces in the dialer rotary group can be used to place outgoing calls.

The **ip unnumbered** interface configuration command specifies that the IP address of loopback interface 1 is to be used as the source address for any IP packets that dialer rotary group 20 might generate. The **dialer**

idle-timeout interface configuration command causes a disconnect if 60 seconds elapses without any interesting traffic.

The configuration includes a **dialer map** interface configuration command for each remote router that the central-site access router might dial. The **ip** keyword specifies that the dialer map is to be used for IP packets, the IP address is the next-hop address of the destination that is to be called, and the **name** keyword specifies the host name of the remote router that is to be called. The **modem-script** keyword specifies that the CALL1020 chat script is to be used, and the **system-script** keyword specifies that the REM chat script is to be used. The last value specified by the **dialer map** command is the telephone number for the remote router. The dialer map commands do not specify the **broadcast** keyword, so RIP updates are not sent to the remote sites.

For the Dialer20 interface, the **dialer-group** interface configuration command defines interesting packets to be those packets defined by the corresponding **dial-list** command. Interesting packets cause a call to be made or cause a call to be maintained. In this case, access list 101 defines RIP as uninteresting. (RIP uses User Datagram Protocol [UDP] port 520.) All other packets are defined as interesting.

OSPF Routing Configuration

Each central-site access router uses the following commands to configure OSPF. These commands limit the routes that are redistributed into OSPF to the major Class B static route and any dynamic subnet routes that may exist for currently connected remote sites. Limiting the routes that are redistributed into OSPF simplifies the routing table on the Cisco 4500 significantly.

```
router ospf 110
redistribute static subnets route-map static-to-ospf
redistribute rip subnets route-map rip-to-ospf
passive-interface async 1
...
passive-interface async 16
network 172.19.0.0 0.0.255.255 area 0
distance 210
!
route-map rip-to-ospf permit
match ip address 20
!
access-list 20 permit 172.16.0.0 0.0.255.0
!
route-map static-to-ospf permit
match ip address 21
!
access-list 21 permit 172.16.0.0
```

The **router ospf** global configuration command enables an OSPF routing process and assigns to it a process ID of 110.

The first **redistribute** router configuration command causes static IP routes to be redistributed into OSPF. The **subnets** keyword specifies that subnets are to be redistributed, and the **route-map** keyword specifies that only those routes that successfully pass through the route map named static-to-ospf are to be redistributed. The static-to-ospf route map permits the redistribution of routes that match access list 21. Access list 21 permits only major network 172.16.0.0.

The second **redistribute** router configuration command causes RIP routes to be redistributed into OSPF. The **subnets** keyword specifies that subnets are to be redistributed, and the **route-map** keyword specifies that only those routes that successfully pass through the route map named rip-to-ospf are to be redistributed. The rip-to-ospf route map permits the redistribution of routes that match access list 20. Access list 20 permits

only routes that start with 172.16 and end with .0 (the third octet is wild). In effect, the RIP-TO-OSPF route map allows only subnets that match 172.16.x.0.

For each asynchronous interface, there is a **passive-interface** router configuration command, which means that OSPF routing information is neither sent nor received through the asynchronous interfaces. The **distance** router configuration command assigns the OSPF routing process an administrative distance of 210. This allows the central-site access routers to prefer their static routes (with an administrative distance of 200) over routes learned by OSPF.

Note: When a remote site logs in and a dynamic route is established for it, the other access routers retain their static routes for that remote site. When a remote site logs out, the other access routers do not need to update their routing tables-their routing tables still contain the static routes that are necessary for dialing out to the remote site.

RIP Routing Configuration

Each access router uses the following commands to configure RIP:

```
router rip
timers basic 30 35 0 1
network 172.16.0.0
distribute-list 10 out Dialer20
!
access-list 10 deny 0.0.0.0 255.255.255.255
```

The **timers basic** router configuration adjusts the RIP update, invalid, holddown, and flush timers. The command specifies that RIP updates are to be sent every 30 seconds, that a route is to be declared invalid if an update for the route is not received within 35 seconds after the previous update, that the time during which better routes are to be suppressed is 0 seconds, and that one second must pass before an invalid route is removed from the routing table. These timer adjustments produce the fastest possible convergence when a remote site logs out.

The **network** router configuration command specifies that network 172.16.0.0 is to participate in the RIP routing process. There is no need to propagate RIP routes to the Cisco 1020s, so the **distribute-list out** router configuration command specifies that access list 10 is to be used to control the advertisement of networks in updates. Access list 10 prevents RIP routes from being sent to the remote site.

Static Routing Configuration

The configuration of each central-site access router includes the following commands for configuring static routes to the remote sites:

```
ip route 172.16.0.0 255.255.0.0 Dialer20
```

The first **ip route** global configuration command creates a static route for major network 172.16.0.0 and assigns it to the dialer interface 20. The route, when distributed into OSPF, tells the Cisco 4500 that this central-site access router can get to the remote sites. If the access router goes down, the Cisco 4500 learns that the route is not longer available and removes it from its routing table. This route is redistributed into OSPF by the STATIC-TO-OSPF filter. The first **ip route** command is followed by pairs of static routes, one pair for each remote site:

```
ip route 172.16.2.0 255.255.255.0 172.16.2.1 200
ip route 172.16.2.1 255.255.255.255 Dialer20
...
ip route 172.16.121.0 255.255.255.0 172.16.121.1 200
ip route 172.16.121.1 255.255.255.255 Dialer20
```

In unnumbered IP environments, two static routes are required for each remote site:

- One static route points to the next hop on the dialer map. Note that the "200" makes this route a floating static route, but that it is lower than OSPF routes (which are set to 210 by the **distance** command, earlier in the configuration). This means that a RIP route triggered by a connection to a remote site (whether the connection is initiated by the remote site or the central site) will override the static route. An OSPF update initiated by a remote site that dials in will not override a static route that points to the next hop address on the dialer map.
- One static route that defines the interface at which the next hop can be found (in this case, dialer interface 20). This static route is required for unnumbered interfaces. Note there is no need to make this a floating static route.

Security Issues

The configuration for each central-site access router includes the **login** line configuration command for each asynchronous line and specifies the **local** keyword. This command causes the access router to match the username and password specified by the **username** global configuration command against the username and password that the remote site specifies when it logs in. This security method is required to allow the remote sites to log in and specify their IP addresses.

Configuration File Size

As the number of remote sites increases, the size of the configuration file for each central-site access router might increase to a size at which it can no longer be stored in NVRAM. There are two ways to alleviate this problem:

- Compress the configuration file using the **service compress-config** global configuration command.
- Have the central-site access routers boot using configuration files stored on a Trivial File Transfer Protocol (TFTP) server.

Configuring the Remote Site Routers

With the exception of the host name and the IP address of the Ethernet interface of each remote site router, the configuration of each remote site router is the same. The discussion of the configuration is divided among the following topics:

- Chat Script Configuration for Dialing the Central Site
- Configuring the Asynchronous Interface
- Using the Site Command
- Static Routing Configuration

For the complete configuration, see the section "Router2 Configuration" later in this article.

Chat Script Configuration for Dialing the Central Site

The configuration of each remote router includes the following **chat-script** global configuration commands:

```
chat-script CENTRALDIAL  "" "ATDT 5551111" "CONNECT" "" "name:" "Router2" "word:"
"outthere" ">" "ppp 172.16.2.1"
```

The **chat-script** command defines a chat script named CENTRALDIAL that is used to place calls to the central site. The CENTRALDIAL chat script specifies the telephone number (555-1111) of the central site and the expect-send sequences that guide the modem through the dial-up process. A key feature of the chat script is that when the remote router receives the string **>** (the prompt indicating that the remote site router has successfully logged in to a central-site access router), the remote router sends the EXEC command **ppp 172.16.2.1**, which informs the central-site access router of the remote router's IP address.

Configuring the Asynchronous Interface

The configuration of each remote router includes the following commands that configure the asynchronous interface:

```
interface async 1
 speed 38400
modem-type usr-sport-v32
 dialer rotary-group 1
!
modem-def usr-sport-v32 </tt> "USR Sportster v.32bis" 38400  "" "AT&F1" "OK"
```

The **speed** line configuration command sets the baud rate to 38400 bits per second for both sending and receiving. The **modem-type** command specifies the initialization string sent to the modem when the interface is reset or when a **clear interface async** command is issued. The initialization string is defined by the **modem-def** command for usr-sport-v32. The **dialer rotary-group** interface configuration command assigns asynchronous interface 1 to dialer rotary group 1.

Using the Site Command

The configuration of each remote router includes the following **site** configuration commands:

```
site CENTRAL
dial-on demand
encapsulation ppp
ip address 172.16.1.1 255.255.255.0
routing rip broadcast
dialgroup 1
session-timeout 5
system-script CENTRALDIAL
password secret
max-ports 1
```

The **site** global configuration command defines a remote location that the router can dial in to or that can dial in to this router, or both, and names it CENTRAL. The name is used to authenticate the central site when it dials in.

The **dial-on** site configuration command uses the **demand** keyword to specify that the central site is to be dialed and a connection established only when packets are queued for the central site. The **encapsulation** site configuration command specifies that when the router establishes a connection with the central site, it is to use PPP encapsulation.

The **ip address** interface configuration command associates IP address 172.16.1.1 with the CENTRAL site. Note that IP address 172.16.1.1 is the address of the dialer 20 interface on each of the central-site access routers. The **routing rip** interface configuration command and the **broadcast** keyword specify that when the router is connected to the central site, IP routing updates are to be broadcast, but any incoming IP routing

updates are to be ignored.

The **dialgroup** command specifies that dial group 1 is to be used when connecting to the central site. Earlier in the configuration, the **dialer rotary-group** command assigned asynchronous interface 1 to group 1.

The **session-timeout** site configuration command specifies that if a period of five minutes elapses during which there is no input or output traffic, the router is to close the connection. The **system- script** site configuration command specifies that the CENTRALDIAL chat script is to be used to dial the central site. The **password** site configuration command specifies that when a central-site access router logs in, its password must be the string "secret."

Static Routing Configuration

The configuration of each remote router includes the following **ip route** global configuration commands:

```
ip route 150.10.0.0 172.16.1.1 1
ip route 172.18.0.0 172.16.1.1 1
ip route 172.19.0.0 172.16.1.1 1
ip route 172.21.0.0 172.16.1.1 1
ip route 172.22.0.0 172.16.1.1 1
```

The **ip route** commands establish static IP routes for networks located at the central site, all reachable through a next-hop address of 172.16.1.1, which is the IP address shared by all of the access routers at the central site. All **ip route** commands specify an administrative distance of 1, which is the default.

The Complete Configurations

This section contains the complete configurations for CENTRAL-1 and Router2.

CENTRAL-1 Configuration

The complete configuration for CENTRAL-1 follows. Those portions of the configuration that must be unique to each central-site access router are highlighted in bold.

```
!
version 10.2
service timestamps debug datetime
service timestamps log datetime
service udp-small-servers
service tcp-small-servers
!
hostname CENTRAL-1
!
enable-password as5100
!
username Router2 password 7 071C2D4359
...
username Router121 password 7 0448070918
!
chat-script CALL1020 ABORT ERROR ABORT BUSY TIMEOUT 30 "" "ATDT\T" "CONNECT" \c
chat-script REM TIMEOUT 40 "name:" "CENTRAL" "word:" "secret"
chat-script usrv32bis "" "AT&F1S0=1&d2" "OK" ""
!
interface loopback 0
ip address 172.16.254.3 255.255.255.255
!
```

```
interface loopback 1
ip address 172.16.1.1 255.255.255.0
!
interface ethernet 0
ip address 172.19.1.8 255.255.0.0
!
interface serial 0
no ip address
shutdown
!
interface async 1
ip unnumbered loopback 1
encapsulation ppp
async dynamic address
async dynamic routing
async mode interactive
dialer in-band
dialer idle-timeout 60
dialer rotary-group 20
...
interface async 16
ip unnumbered loopback 1
encapsulation ppp
async dynamic address
async dynamic routing
async mode interactive
dialer in-band
dialer idle-timeout 60
dialer rotary-group 20
!
interface dialer 20
ip unnumbered loopback 1
encapsulation ppp
dialer in-band
dialer idle-timeout 60
dialer fast-idle 60
dialer map ip 172.16.2.1 name Router2 modem-script CALL1020 system-script REM 5551234
...
dialer map ip 172.16.121.1 name Router121 modem-script CALL1020 system-script REM 5555678
dialer-group 3
!
router ospf 110
redistribute static subnets route-map static-to-ospf
redistribute rip subnets route-map rip-to-ospf
passive-interface async 1
...
passive-interface async 16
network 172.19.0.0 0.0.255.255 area 0
distance 210
!
router rip
timers basic 30 35 0 1
network 172.16.0.0
distribute-list 10 out Dialer20
!
ip default-gateway 172.19.1.10
!
ip route 172.16.0.0 255.255.0.0 Dialer20
ip route 172.16.2.0 255.255.255.0 172.16.2.1 200
ip route 172.16.2.1 255.255.255.255 Dialer20

...
ip route 172.16.121.0 255.255.255.0 172.16.121.1 200
ip route 172.16.121.1 255.255.255.255 Dialer20
```

```
access-list 10 deny 0.0.0.0 255.255.255.255
access-list 20 permit 172.16.0.0 0.0.255.0
access-list 21 permit 172.16.0.0
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 520
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
route-map rip-to-ospf permit
match ip address 20
!
route-map static-to-ospf permit
match ip address 21
!
snmp-server community public RO
snmp-server community private RW
dialer-list 3 list 101
!
line con 0
line 1 16
login local
modem inout
script reset usrv32bis
transport input all
rxspeed 38400
txspeed 38400
flowcontrol hardware
line aux 0
transport input all
line vty 0 4
exec-timeout 20 0
password cisco
login
!
end
```

Router2 Configuration

The complete configuration for Router2 follows. Those portions of the configuration that must be unique to each remote site router are highlighted in bold.

```
version 1.1(2)
!
hostname Router2
!
enable-password cisco-a
!
chat-script CENTRALDIAL "" "ATDT 5551111" "CONNECT" "" "name:" "Router2" "word:"
"outthere" ">" "ppp 172.16.2.1"
!
interface ethernet 0
ip address 172.16.2.1 255.255.255.0
!
interface async 1
speed 38400
modem-type usr-sport-v32
dialer rotary-group 1
!
site CENTRAL
dial-on demand
encapsulation ppp
ip address 172.16.1.1 255.255.255.0
routing rip broadcast
dialgroup 1
session-timeout 5
```

```
system-script CENTRALDIAL
password secret
max-ports 1
!
modem-def usr-sport-v32 "USR Sportster v.32bis" 38400  "" "AT&F1" "OK"
!
ip route 150.10.0.0 172.16.1.1 1
ip route 172.18.0.0 172.16.1.1 1
ip route 172.19.0.0 172.16.1.1 1
ip route 172.21.0.0 172.16.1.1 1
ip route 172.22.0.0 172.16.1.1 1
```

Summary

This case study shows that it is possible to scale dial-on-demand routing to accommodate large dial-up networks. If, in the future, the number of remote sites exceeds the capacity of the 48 asynchronous interfaces, additional routers can be installed without modifying the routing strategy. Although this case study focuses on asynchronous media, many of the techniques can be applied to other dial-up technologies, such as ISDN.