



Configuring Large-Scale Dial-Out

This chapter describes how to configure large-scale dial-out. It includes the following main sections:

- [Large-Scale Dial-Out Overview](#)
- [How to Configure Large-Scale Dial-Out](#)
- [Monitoring and Maintaining the Large-Scale Dial-Out Network](#)
- [Configuration Examples for Large-Scale Dial-Out](#)

Consider these restrictions when configuring large-scale dial-out:

- Large-scale dial-out supports only IP over PPP encapsulation.
- Large-scale dial-out does not support tunneling protocols such as Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP).
- Virtual profiles depend on PPP authentication; however, this authentication can create a problem for Ascend devices, which do not allow devices to authenticate them when answering a call (bidirectional authentication is not supported).
- The IP address of the remote device must be known before dialing out. Large-scale dial-out does not support dynamic IP address assignment.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the “Using Cisco IOS Software” chapter.

For a complete description of the commands mentioned in this chapter, refer to [Cisco IOS Dial Technologies Command Reference](#), Release 12.2. To locate documentation of other commands that appear in this chapter, use [Cisco IOS Command Reference Master Index](#) or search online.

Large-Scale Dial-Out Overview

In previous dial-on-demand routing (DDR) networking strategies, only incoming calls could take advantage of features such as dialer and virtual profiles, Multichassis Multilink PPP (MMP) support, and the ability to use an authentication, authorization, and accounting (AAA) server to store attributes. MMP allows network access servers to be stacked together and appear as a single network access server chassis so that if one network access server fails, another network access server in the stack can accept calls. MMP also provides stacked network access servers access to a local Internet point of presence (POP) using a single telephone number. This capability allows for easy expansion and scalability and for assured fault tolerance and redundancy. Now, with large-scale dial-out, these features are available for both outgoing and incoming calls.

Large-scale dial-out eliminates the need to configure dialer maps on every network access server for every destination. Instead, you create remote site profiles that contain outgoing call attributes (telephone number, service type, and so on) on the AAA server. The profile is downloaded by the network access server when packet traffic requires a call to be placed to a remote site.

Additionally, large-scale dial-out addresses congestion management by seeking an uncongested, alternative network access server within the same POP when the designated primary network access server experiences port congestion.

Large-scale dial-out also enables scalable dial-out service to many remote sites across one or more Cisco network access servers or Cisco routers. This capability is especially beneficial to both Internet service providers (ISPs) and large-scale enterprise customers because it can simplify network configuration and management. Large-scale dial-out streamlines activities such as service maintenance and scheduled activities like application upgrades from a centralized location. Large enterprise networks such as those used by retail stores, supermarket chains, and franchise restaurants can use large-scale dial-out to easily update daily prices and inventory information from a central server to all branch locations in one process, using the same network access servers that they currently use for dial-in functions.

Additional benefits of using large-scale dial-out include the following:

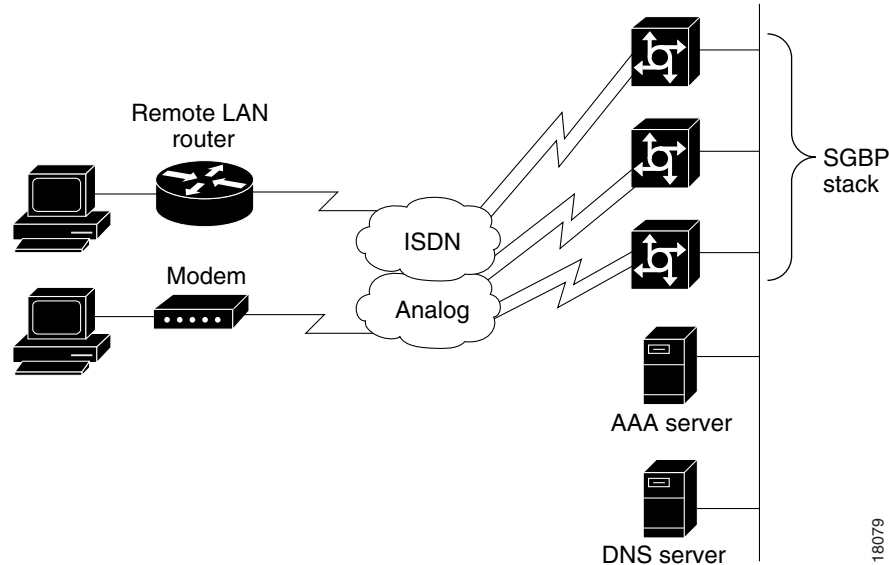
- Allows dialing the same router from any router in a stack group. Using a primary network access server, you can configure static routes for a given remote host or network. If the primary network access server is congested or has no links available, it will search for an alternate server within the stack, and force that server to dial out.
- Eliminates the need to configure dialer maps in individual network access servers. The user profiles, along with dial parameters, can be centrally stored on an AAA server such as a Cisco Secure Access Control Server (ACS).
- Supports extended TACACS (also TACACS+), RADIUS using Cisco attribute-value (AV) pairs, and the Ascend proprietary RADIUS extension for dial-out operation.
- Provides a way to associate an IP address with a user name and user profile using the static route and host name association features. If there are no names on the IP static route, the Domain Name System (DNS) support function can be used to determine the user name that is associated with the IP address. If a name is not found, the destination IP address is used for the name.
- Allows dynamic static routes to be configured on the centralized AAA server, that is, static routes stored centrally on an AAA server that can be dynamically downloaded by the router as needed.
- Provides support for MMP and the Stack Group Bidding Protocol (SGBP). SGBP unites each Cisco access server in a virtual stack, which enables the access servers to become virtually tied together. If all ports on a given network access server are already being used, the other network access servers on the stack can be used for outbound calls. Single calls and multilink calls are now supported across the multichassis stack group.
- Supports dial-out over an asynchronous line, when a chat script is configured.
- Allows ports to be reserved for dial-in and dial-out.

Large-scale dial-out enables scalable dial-out service; that is, configuration information is stored in a central server, and many network access servers can access this information using either the RADIUS or extended TACACS protocols. One or more network access servers can advertise summary routes to the remote destinations and then dynamically download the dial-out profile configurations as needed.

Large-scale dial-out also allows dialing the same remote network or host from any router in a stack group. You configure static routes for a particular remote host or network on a router in a stack group that you designate as the primary network access server for that remote network or host. When a primary network access server experiences port congestion, it searches for an alternate network access server within the stack group to dial out and, when found, forces the alternate to dial the remote network.

[Figure 96](#) illustrates the large-scale dial-out solution.

Figure 96 Large-Scale Dial-Out Components



Large-scale dial-out relies on per-user static routes in AAA and redistributed static and redistributed connected routes to put better routes pointing to the same remote on the alternate network access server. You can use any routing protocol that supports redistributing static and connected routes and that supports Flash memory updates when a routing topology changes. The Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocols are recommended.

Next Hop Definition

A next hop address or remote name that you define is used in an AAA server lookup to retrieve the user profile from the remote network or host. The name is passed to the AAA server by the router software.

Static Routes

Static routes can be dynamically downloaded from an AAA server by the network access servers or can be manually configured on the network access servers.

Dynamic static routes are installed on the network access server by an AAA server. The routes are downloaded at system startup and updated periodically, so that route changes are reflected within a configurable interval of time. Large-scale dial-out allows multiple AAA transactions with 50 static routes per AAA server transaction. There is no set limit for the number of AAA server transactions which can be configured, however configuring too many transactions may impact the performance of your network. Performance effects will depend on the configurations and platforms used in your network.

Stack Groups

The network access server stack group redistributes the routes of the remote networks. If the number is large, the routes are summarized. Packets destined for remote networks are routed to the primary network access server for the remote network.

If the static route that points to the next hop of the network access server has a name, that name with the -out suffix attached becomes the profile name. If no profile name is configured in the route statement that defines the remote location, the router can use reverse DNS lookup to map the IP route to a profile name. The next hop address on the static route is used in reverse DNS to obtain the name of the remote network. This name is then used in the AAA server lookup to retrieve the remote user profile. If no name is returned by DNS, the network access server uses the destination IP address with the -out suffix appended as the name.

If the primary network access server is congested, an alternate network access server may dial out. The primary network access server initiates stack group bidding for the outgoing call. The least congested network access server wins the bid and downloads the user profile. After a call is connected on an alternate network access server, a better per-user route from the AAA profile is installed on the alternate network access server. Subsequent packets destined for the remote network are routed to the alternate network access server while the call is connected. Packets stored in the dialer hold queue on the primary network access server are switched to the alternate network access server when the new route is distributed to the primary network access server.

How to Configure Large-Scale Dial-Out

To configure large-scale dial-out perform the tasks in the following sections:

- [Complying with Large-Scale Dial-Out Prerequisites](#) (Required)
- [Establishing the Route to the Remote Network](#) (As required)
- [Enabling AAA and Static Route Download](#) (Required)
- [Enabling Access to the AAA Server](#) (Required)
- [Enabling Reverse DNS](#) (Required)
- [Enabling SGBP Dial-Out Connection Bidding](#) (Required)
- [Defining a User Profile](#) (Required)

See the section “[Monitoring and Maintaining the Large-Scale Dial-Out Network](#)” later in this chapter for tips on maintaining large-scale dial-out. See the examples in the section “[Configuration Examples for Large-Scale Dial-Out](#)” at the end of this chapter for ideas on how you can implement large-scale dial-out in your network.

Complying with Large-Scale Dial-Out Prerequisites

The following prerequisites apply to large-scale dial-out:

- Virtual profiles depend on PPP authentication; therefore the network access server, the remote device, or both must authenticate the connection to use virtual profiles.
- You must configure SGBP to allow a primary network access server that is congested or otherwise unable to dial out to select an alternate network access server to dial out. Configure SGBP using the **sgbp group** and **sgbp member** global configuration commands before enabling the stack group to bid for dial-out connection. Configuring SGBP is described in the chapter “[Configuring Multichassis Multilink PPP](#)” in this publication. The *Cisco IOS Dial Technologies Command Reference* describes the commands to configure a stack group.

Additionally, all members of the stack group must be in the same routing autonomous system, and the **redistribute static** and **redistribute connected** commands must already be configured. The stack group supports all routing protocols, but routing protocols such as EIGRP and OSPF, which support redistributing static and connected routes and Flash memory updates when topology changes, are recommended.

- You must configure AAA network security services using the **aaa new-model**, **aaa authentication**, **aaa authorization**, and **aaa accounting** global configuration commands. For more information about AAA, see the chapter “AAA Overview” in the *Cisco IOS Security Configuration Guide*. The *Cisco IOS Security Command Reference* describes the commands to configure AAA.

You will also need to configure your network access server to communicate with the applicable security server, either an extended TACACS or RADIUS daemon.

If you are using RADIUS and Ascend attributes, use the **non-standard** keyword with the **radius-server host** command to enable your Cisco router, acting as a network access server, to recognize that the RADIUS security server is using a vendor-proprietary version of RADIUS. Use the **radius-server key** command to specify the shared secret text string used between your Cisco router and the RADIUS server. For more information, see the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*.

If you are using extended TACACS, use the **tacacs-server host** command to specify the IP address of one or more extended TACACS daemons. Use the **tacacs-server key** command to specify the shared secret text string used between your Cisco router and the extended TACACS daemon. For more information, see the chapter about configuring extended TACACS in the *Cisco IOS Security Configuration Guide*.

Establishing the Route to the Remote Network

The task in this section is optional; you only need to perform it when routes will not be downloaded statically from the AAA server.

To establish a route to the remote network or host (next hop) that holds the user profile, use the **ip route** command in global configuration mode:

| Command | Purpose |
|---|--|
| Router(config)# ip route <i>network-number</i> [<i>network-mask</i>] { <i>address</i> <i>interface</i> } [<i>distance</i>] [name <i>name</i>] | Establishes a static route to a remote network to obtain a user profile. |

The name you define is used in an AAA server lookup to retrieve the AAA profile of the remote network.

Enabling AAA and Static Route Download

AAA network security must be enabled before you perform the tasks in this section. For more information about enabling AAA, see the chapter “AAA Overview” in the *Cisco IOS Security Configuration Guide*.

Enabling the static route download feature allows static routes to be configured at a centrally located AAA server. Static routes are downloaded when the system is started, and you define a period of time between route updates when you enable the feature.

**Note**

Static route download is not mandatory for the large-scale dial-out feature; however, it makes configuration of static routes more manageable by allowing the configuration to be centralized on a server.

To enable the static route download feature, use the following commands in global configuration mode:

| | Command | Purpose |
|--------|---|---|
| Step 1 | Router(config)# aaa new-model | Enables the AAA server. |
| Step 2 | Router(config)# aaa route download [time] | Downloads static routes from the AAA server periodically using the host name of the router. |
| Step 3 | Router(config)# aaa authorization configuration default [radius tacacs+] | Downloads configuration information from the AAA server. |

Use the **show ip route** command to see the routes installed by these commands.

Enabling Access to the AAA Server

To configure the dialer interface to access the AAA server and retrieve the user profile, use the following command in interface configuration mode for a dialer rotary group leader:

| Command | Purpose |
|--------------------------------------|---|
| Router(config-if)# dialer aaa | Allows the dialer to use the AAA server to locate profiles for dialing information. |

Enabling Reverse DNS

To instruct the dialer to use reverse DNS on dial out, use the following command in interface configuration mode:

| Command | Purpose |
|--------------------------------------|--|
| Router(config-if)# dialer dns | Uses reverse DNS to obtain the name of the user profile of the remote network. |

The user profile name passed to the AAA server by the system is *reverse-dns-name-out*; the -out suffix is automatically appended to the DNS name and is required to create unique dial-out and dial-in profiles.

Enabling SGBP Dial-Out Connection Bidding

You must configure SGBP before performing the tasks in this section. The chapter “Configuring Multichassis Multilink PPP” in this publication describes the tasks you perform to configure a stack group.

To configure stack group bidding, use the following command in global configuration mode:

| Command | Purpose |
|---------------------------------------|--|
| Router(config)# sgbp dial-bids | Allows the stack group to bid for the dial-out call. |

Once the stack group has been configured and enabled for dial-out connection bidding, configure the dialer interface to search for an alternate network access server in the event of port congestion. Use the following commands in interface configuration mode:

| | Command | Purpose |
|---------------|--|--|
| Step 1 | Router(config-if)# dialer congestion-threshold <i>links</i> | Forces the dialer to search for another uncongested system in the stack group. |
| Step 2 | Router(config-if)# dialer reserved-links { <i>dialin-link</i> <i>dialout-link</i> } | Reserves links for dial in and dial-out. |

See the section “[Stack Group and Static Route Download Configuration Example](#)” at the end of this chapter for an example of how to configure stack groups and static routes.

Defining a User Profile

Attributes are used to define specific AAA elements in a user profile. Large-scale dial-out supports a subset of Ascend AV pairs and RADIUS attributes, as well as a map class attribute that provides outbound dialing services, as described in [Table 36](#).

The only required attribute is the Cisco AV pair `outbound:dial-number`; all others are optional. If the AAA server does not support Cisco AV pairs, attribute `#227, Ascend-Dial-Number`, can be substituted. If there are equivalent Cisco AV pairs and Ascend-specific attributes, Cisco recommends using the Cisco AV pairs.

For additional information about defining user profiles, see the chapter “RADIUS Attribute-Pairs” in the *CiscoSecure ACS for Windows NT User Guide 2.0* publication and the chapter “TACACS+ Attribute-Value Pairs” in the *Cisco IOS Security Configuration Guide*.

For an example of a user profile that uses the supported attributes, see the section “[User Profile on an Ascend RADIUS Server for NAS1 Example](#)” at the end of this chapter.



Note

For the attributes listed in Table 4, the value of a string is 0 to 253 octets; the value of an integer is a 32-bit value ordered high byte first.

Table 36 Large-Scale Dial-Out Outbound Service Attributes

| Number | Attribute | Description |
|------------------------|---------------------------|--|
| Ascend AV Pairs | | |
| #214 | Ascend-Send-Secret | <p>Specifies the password that the network access server uses when the remote site challenges the network access server to authenticate using either Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).</p> <p>Cisco AV Pair: None</p> <p>TACACS+ Support:</p> <pre>service = outbound { send-secret = VALUE }</pre> <p>Value: Password string</p> <p>Note The password is encrypted. This attribute requires a special RADIUS daemon that supports CHAP or PAP authentication.</p> |
| #227 | Ascend-Dial-Number | <p>Defines the number to dial.</p> <p>Cisco AV Pair: cisco-avpair="outbound:dial-number=VALUE"</p> <p>TACACS+ Support:</p> <pre>service = outbound { dial-number = VALUE }</pre> <p>Value: Dial string</p> <p>Note This attribute defines the plain dial number. It can be used in different profiles, whereas the callback-dialstring attribute is only for callbacks.</p> |

Table 36 Large-Scale Dial-Out Outbound Service Attributes (continued)

| Number | Attribute | Description |
|--------|------------------|---|
| #231 | Ascend-Send-Auth | <p>Specifies the authentication protocol that the network access server requests when initiating a connection using PPP. The answering side of the connection determines which authentication protocol, if any, that the connection uses. The network access server will refuse to negotiate PAP if CHAP is selected, but will negotiate CHAP if PAP is selected.</p> <p>Cisco AV Pair:</p> <pre>cisco-avpair="outbound:send-auth=VALUE"</pre> <p>TACACS+ Support:</p> <pre>service = outbound { send-auth = none/pap/chap }</pre> <p>Value:</p> <p>0: Send-Auth-None 1: Send-Auth-PAP 2: Send-Auth-CHAP</p> |
| #247 | Ascend-Data-SVC | <p>Specifies the type of data service that the link uses for outgoing calls.</p> <p>Cisco AV Pair:</p> <pre>cisco-avpair="outbound:data-service=VALUE"</pre> <p>TACACS+ Support:</p> <pre>service = outbound { data-service = VALUE }</pre> <p>Value:</p> <p>0: Switched-Voice-Bearer</p> |
| #248 | Ascend-Force-56 | <p>Determines whether the network access server uses only the 56K portion of a channel, even when all 64K appear to be available.</p> <p>Cisco AV Pair:</p> <pre>cisco-avpair="outbound:force-56=VALUE"</pre> <p>TACACS+ Support:</p> <pre>service = outbound { force-56 = VALUE }</pre> <p>Value:</p> <p>0: Force-56-No 1: Force-56-Yes</p> |

Table 36 Large-Scale Dial-Out Outbound Service Attributes (continued)

| Number | Attribute | Description |
|---------------------------------|------------------------|--|
| RADIUS (IETF) Attributes | | |
| #10 | Framed-Routing | <p>Indicates a routing method when a router is used to access a network.</p> <p>Cisco AV Pair:</p> <p>None</p> <p>TACACS+ Support:</p> <pre>service = outbound { routing = VALUE }</pre> <p>Value:</p> <p>0: None 1: Broadcast 2: Listen 3: Broadcast-Listen</p> <p>Note This attribute is currently supported only for PPP service.</p> |
| #19 | Callback-Number | <p>Defines a dialing string to be used for call back. (Service is both outbound and PPP.)</p> <p>Cisco AV Pair:</p> <pre>cisco-avpir="outbound:callback-dialstring=VALUE"</pre> <p>TACACS+ Support:</p> <p>Equivalent to the existing callback-dialstring attribute.</p> <p>Value:</p> <p>Dial string</p> <p>Note This is an alternate way of setting a callback number using a standard RADIUS attribute.</p> |

Table 36 Large-Scale Dial-Out Outbound Service Attributes (continued)

| Number | Attribute | Description |
|----------------------------|---------------|--|
| #61 | NAS-Port-Type | <p>Indicates the type of physical port that the network access server is using to authenticate the user.</p> <p>Cisco AV Pair: None</p> <p>TACACS+ Support: None</p> <p>Value: 0: Asynchronous 1: Synchronous 2: ISDN-Synchronous</p> <p>Note This attribute is currently supported only for PPP service.</p> |
| Map Class Attribute | | |
| (unnumbered) | map-class | <p>Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out.</p> <p>Cisco AV Pair: <code>cisco-avpair="outbound:map-class=VALUE"</code></p> <p>TACACS+ Support:</p> <pre>service = outbound { map-class = VALUE }</pre> <p>Value: Name string, which must match the name of a map class on the dial-out network access server.</p> |

Monitoring and Maintaining the Large-Scale Dial-Out Network

To monitor and maintain a large-scale dial-out network, use any of the following commands in EXEC mode:

| Command | Purpose |
|---|--|
| Router> clear dialer sessions | Removes all dialer sessions and disconnects links. |
| Router> clear ip route download {* <i>network-number</i> <i>network-mask</i> reload } | Removes all or specified IP routes on the router. With the reload option, forces reload of dynamic static routes before the update timer expires. |
| Router> show dialer sessions | Displays all dialer sessions. |
| Router> show ip route [static [download]] | Displays all static IP routes or those installed using the AAA route download function. |

Configuration Examples for Large-Scale Dial-Out

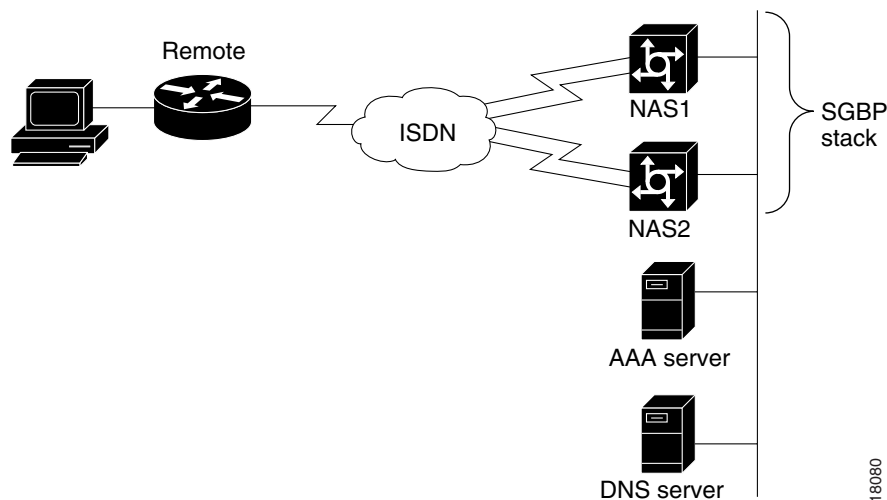
The following sections provide examples of how you can configure large-scale dial-out in your network:

- [Stack Group and Static Route Download Configuration Example](#)
- [User Profile on an Ascend RADIUS Server for NAS1 Example](#)
- [Asynchronous Dialing Configuration Examples](#)

Stack Group and Static Route Download Configuration Example

The following example configures NAS1 as the primary network access server and NAS2 as the secondary network access server, in a stack group for dial-out. The remote router is configured to answer calls. [Figure 97](#) illustrates the configuration.

Figure 97 Stack Group and Static Route Download Configuration



18080

At the console for NAS1, ping 20.1.1.1. This action creates a multilink bundle with two links. NAS1 dials out the first link, and NAS2 dials out the second link. The router named Remote is using the CHAP host name echo-8.cisco.com.

A user profile for NAS1 on an Ascend RADIUS server is listed in the section [“User Profile on an Ascend RADIUS Server for NAS1 Example”](#) later in this chapter.

Primary Network Access Server Configuration for NAS1

```

version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname NAS1
!
aaa new-model
aaa authentication ppp default radius local
aaa authorization network default radius none
aaa authorization configuration default radius
aaa route download 720
enable password 7 1236173C1B0F
!
username NAS2 password 7 05080F1C2243
username NAS1 password 7 030752180500
username dialbid password 7 121A0C041104
username echo-8.cisco.com password 7 02050D480809
ip subnet-zero
ip domain-name cisco.com
ip name-server 172.31.2.132
ip name-server 172.22.30.32
!
virtual-profile virtual-template 2
!
sgbp group dialbid
sgbp seed-bid offload
sgbp member NAS2 172.21.17.17
sgbp dial-bids
isdn switch-type basic-5ess
!
!
interface Ethernet 0
 ip address 172.21.17.18 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 media-type 10BaseT
 no cdp enable
!
interface Virtual-Template 1
 ip address 10.1.1.1 255.255.255.252
 no ip directed-broadcast
!
interface Virtual-Template 2
 ip unnumbered Virtual-Template 1
 no ip directed-broadcast
 ppp multilink
 multilink load-threshold 1 outbound
!
interface BRI 0
 description PBX 60043
 no ip address
 no ip directed-broadcast
 encapsulation ppp

```

```

dialer rotary-group 1
isdn switch-type basic-5ess
no fair-queue
!
interface Dialer 1
ip unnumbered Ethernet 0
no ip directed-broadcast
encapsulation ppp
no ip mroute-cache
dialer in-band
dialer dns
dialer aaa
dialer hold-queue 5
dialer congestion-threshold 5
dialer reserved-links 1 0
dialer-group 1
no fair-queue
ppp authentication chap callin
ppp multilink
!
router eigrp 200
 redistribute connected
 redistribute static
 network 172.21.0.0
!
ip default-gateway 172.21.17.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.21.17.1
!
dialer-list 1 protocol ip permit
radius-server host 172.31.61.87 auth-port 1645 acct-port 1646
radius-server key foobar
!
end

```

Secondary Network Access Server Configuration for NAS2

```

version 12.0
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
!
hostname NAS2
!
boot system flash
aaa new-model
aaa authentication ppp default radius local
aaa authorization network default radius none
aaa authorization configuration default radius
enable password 7 022916700202
!
username NAS1 password 7 104D000A0618
username dialbid password 7 070C285F4D06
username echo-8.cisco.com password 7 0822455D0A16
ip subnet-zero
ip domain-name cisco.com
ip name-server 172.22.30.32
ip name-server 172.31.2.132
!
virtual-profile virtual-template 2
!
sgbp group dialbid
sgbp member NAS1 172.21.17.18

```

```
sgbp dial-bids
isdn switch-type basic-5ess
!
interface Ethernet 0
 ip address 172.21.17.17 255.255.255.0
 no ip directed-broadcast
 media-type 10BaseT
!
interface Virtual-Template 1
 ip address 10.1.1.1 255.255.255.252
 no ip directed-broadcast
!
interface Virtual-Template 2
 ip unnumbered Virtual-Template 1
 no ip directed-broadcast
 ppp multilink
 multilink load-threshold 1 outbound
!
interface BRI 0
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 dialer rotary-group 0
 isdn switch-type basic-5ess
 no fair-queue
!
interface Dialer 0
 ip unnumbered Ethernet 0
 no ip directed-broadcast
 encapsulation ppp
 dialer in-band
 dialer dns
 dialer aaa
dialer hold-queue 5
dialer congestion-threshold 5
dialer reserved-links 1 0
dialer-group 1
 no fair-queue
 ppp authentication chap callin
 ppp multilink
!
router eigrp 200
 redistribute connected
 redistribute static
 network 172.21.0.0
!
ip default-gateway 172.21.17.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.21.17.1
!
dialer-list 1 protocol ip permit
!
radius-server host 172.31.61.87 auth-port 1645 acct-port 1646
radius-server key foobar
!
end
```

Remote Router Configuration

```
version 12.0
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname Remote
!
boot system flash
enable password 7 002B012D0D5F
!
username dialbid password 7 14141B180F0B
ip subnet-zero
no ip domain-lookup
!
isdn switch-type basic-5ess
!
interface Loopback 0
 ip address 172.31.229.41 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback 1
 ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback 2
 ip address 10.1.2.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback 3
 ip address 10.3.1.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet 0
 ip address 172.21.12.15 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface BRI 0
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer rotary-group 3
 dialer-group 1
 isdn switch-type basic-5ess
 no fair-queue
!
interface Dialer 3
 ip unnumbered Loopback 0
 no ip directed-broadcast
```

```

encapsulation ppp
no ip route-cache
no ip mroute-cache
dialer in-band
dialer idle-timeout 10000
dialer-group 1
no fair-queue
ppp authentication chap callin
ppp chap hostname echo-8.cisco.com
ppp chap password 7 045802150C2E
ppp multilink
!
ip default-gateway 172.21.12.1
ip classless
ip route 0.0.0.0 0.0.0.0 1.1.1.1
!
dialer-list 1 protocol ip permit

```

User Profile on an Ascend RADIUS Server for NAS1 Example

The following example shows a dial-out profile and a static route download profile in AAA. The dial-out profile username must have “-out” appended to it. The static route download profile username always has “-N” appended. The router downloads NAS1-1, NAS1-2, through NAS1-N. When NAS1-N fails, the router does not try NAS1-N+1. The static route download profile cannot have more than 50 static routes defined.

```

echo-8.cisco.com-out Password = "cisco", User-Service-Type = Outbound-User
cisco-avpair = "outbound:addr=172.31.229.41",
cisco-avpair = "outbound:dial-number=60039",

NAS1-1 Password = "cisco" User-Service-Type = Outbound-User,
cisco-avpair = "ip:route=10.1.3.0 255.255.255.0 172.31.229.41 200",
cisco-avpair = "ip:route=10.1.2.0 255.255.255.0 172.31.229.41 200",
cisco-avpair = "ip:route=10.1.1.0 255.255.255.0 172.31.229.41 200",
cisco-avpair = "ip:route=172.31.229.41 255.255.255.255 Dialer1 200 name
echo-8.cisco.com"

```



Note

Note that all text between quotation marks must be typed on one line.

Static routes can also be defined using the Framed-Route Internet Engineering Task Force (IETF) standard. The following example shows how the previous example for NAS1 would look using the Framed-Route IETF standard:

```

NAS1-1 Password = "cisco" User-Service-Type = Outbound-User,
Framed-Route = "10.1.3.0/24 172.31.229.41.200",
Framed-Route = "10.1.2.0/24 172.31.229.41.200",
Framed-Route = "10.1.1.0/24 172.31.229.41.200",
Framed-Route = "172.31.229.41/32 Dialer1 200 name echo-8.cisco.com"

```

Asynchronous Dialing Configuration Examples

Large-scale dial-out supports dialing out using an asynchronous line. This type of dialing requires that a chat script be configured and that the **script dialer** command be configured in the line commands for any asynchronous interface that may be dialing out. The following examples are provided in this section:

- [Asynchronous Dialing Example](#)
- [Asynchronous and Synchronous Dialing Example](#)

Asynchronous Dialing Example

The following example shows an asynchronous dialing configuration:

```
chat-script dial "" "ATZ" OK "ATDT\T" TIMEOUT 60 CONNECT
!
interface Async 1
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  dialer in-band
  dialer rotary-group 0
  async dynamic address
  async dynamic routing
  async mode dedicated
  no cdp enable
!
interface Dialer 0
  ip address 172.21.30.32 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  no ip mroute-cache
  bandwidth 64
  dialer in-band
  dialer idle-timeout 60
  dialer enable-timeout 10
  dialer hold-queue 50
  dialer-group 1
  no cdp enable
!
line 1
  script dialer dial
  modem InOut
  transport input all
```

Asynchronous and Synchronous Dialing Example

The following example creates a dialer rotary group for the asynchronous interfaces and a dialer rotary group for the PRI interfaces. Any dial-in or dial-out reservations are applied only to the PRI dialer interface. In the following configuration example:

- Destinations that require modem calls have static routes that point to Dialer 0.
- Destinations that require digital connections have static routes that point to Dialer 1.
- The **dialer reserved-links** command applies to all connections made over the PRI interfaces in dialer rotary group 1, even if they come from an asynchronous interface.

```
chat-script dial "" "ATZ" OK "ATDT\T" TIMEOUT 60 CONNECT
!
interface Serial 0:23
  no ip address
  no ip directed-broadcast
  no keepalive
  dialer rotary-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no cdp enable
!
interface Async 1
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  dialer in-band
  dialer rotary-group 0
  async dynamic address
  async dynamic routing
  async mode dedicated
  no cdp enable
!
interface Dialer 0
  ip address 172.21.30.32 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  no ip mroute-cache
  bandwidth 64
  dialer in-band
  dialer dns
  dialer aaa
  dialer idle-timeout 60
  dialer enable-timeout 10
  dialer hold-queue 50
  dialer-group 1
  no cdp enable
!
interface Dialer 1
  ip address unnumbered eth0
  no ip directed-broadcast
  dialer in-band
  dialer dns
  dialer aaa
  dialer reserved-links 22 0
  no cdp enable
!
line 1
  script dialer dial
  modem InOut
  transport input all
```

