

# Large Scale Dialout

---

## Feature Summary

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 allows for easy expansion and scalability, as well as assured fault tolerance and redundancy. Now with large scale dialout, these features are available for both outgoing and incoming calls.

Large scale dialout eliminates the need to configure dialer maps on every network access server for every destination. Instead, you create remote site profiles containing 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 dialout 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.

As an added benefit, large scale dialout enables scalable dial-out service to many remote sites across one or more Cisco network access servers or Cisco routers. This is especially beneficial to both Internet service providers and large scale enterprise customers because it can simplify network configuration and management. Large scale dialout 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 dialout 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 they currently use for dial in functions.

## Benefits

Benefits of using large scale dialout 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 CiscoSecure Access Control Server (ACS).
- Supports Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS) using Cisco AV pairs, and the Ascend proprietary RADIUS extension for dialout 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). 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 as well as multilink calls are now supported across the multichassis stack group.
- Supports dialout over an asynchronous line, when a chat script is configured.
- Ports can be reserved for dial in and dialout.

## List of Terms

**Authentication, authorization, and accounting server (AAA)**—Typically a CiscoSecure ACS, TACACS+, or RADIUS server.

**Domain Name System (DNS)**—System used in the Internet for translating names of network nodes into addresses.

**Dynamic static route (DSR)**—A static route that has been installed by means other than configuration, such as AAA server authorization.

**Multichassis Multilink PPP (MMP)**—Extends Multilink PPP support across multiple routers and access servers. MMP enables multiple routers and access servers to operate as a single, large dial-up pool, with a single network address and ISDN access number. MMP correctly handles packet fragmenting and reassembly when a user connection is split between two physical access devices.

**Network access server**—This device typically has PSTN interfaces and answers or dials PSTN calls.

**Oversubscription**—Number of users serviced by a network access server is larger than the number of ports available.

**Point of presence (POP)**—A physical location where interexchange carrier installed equipment interconnects with a local exchange carrier.

**Port congestion**—Occurs when the network access server resources have been consumed to predetermined level. In the extreme case, an network access server with all ports connected is experiencing a Port Congested error condition.

**Primary network access server**—Each remote site has a designated primary network access server. The primary network access server is the first choice for dialout operations.

**Public Switched Telephone Network (PSTN)**—Traditional telephone or ISDN network.

**Secondary network access server**—An alternative choice for dialout when port congestion occurs.

**Stack Group Bidding Protocol (SGBP)**—A critical component used in multichassis, multilink sessions. The 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 device CPU should be in charge of running the multilink session and packet reassembly. The goal of SGBP is to find a common place to forward the links and ensure that this destination has enough system processor space to perform the segmentation and packet reassembly.

## Restrictions

Consider these restrictions when configuring large scale dialout:

- Large scale dialout only supports IP over PPP encapsulation.
- Large scale dialout does not support tunneling protocols such as Layer 2 Forwarding Protocol (L2F) or Layer 2 Tunneling Protocol (L2TP).
- Virtual profiles depend on PPP authentication; however, this will 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 prior to dialing out. Large scale dialout does not support dynamic IP address assignment.

## Platforms

This feature is supported on these platforms:

- Cisco 2500 series routers
- Cisco 2600 series routers
- Cisco 3600 series routers
- Cisco 4000-M, 4500-M, 4700-M routers
- Cisco 4500 series routers
- Cisco 7200 series routers
- Cisco 7500 series routers
- Cisco AS5200 series access servers
- Cisco AS5300 series access servers
- Cisco AS5800 series access servers

## Prerequisites

The following prerequisites apply to large scale dialout:

- 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 dialout connection. Configuring SGBP is described in the *Dial Solutions Configuration Guide*, in the section “Configuring Multichassis Multilink PPP.” The *Dial Solutions Command Reference* describes the commands you use 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, refer to the “AAA Overview” chapter in the Cisco IOS Release 12.0 *Security Configuration Guide*. The Cisco IOS Release 12.0 *Security Command Reference* describes the commands you use to configure AAA.

You will also need to configure your network access server to communicate with the applicable security server, either a 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, refer to the “Configuring RADIUS” chapter in the Cisco IOS Release 12.0 *Security Configuration Guide*.

If you are using TACACS+, use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons. Use the **tacacs-server key** command to specify the shared secret text string used between your Cisco router and the TACACS+ daemon. For more information, refer to the “Configuring TACACS+” chapter in the Cisco IOS Release 12.0 *Security Configuration Guide*.

## Supported MIBs and RFCs

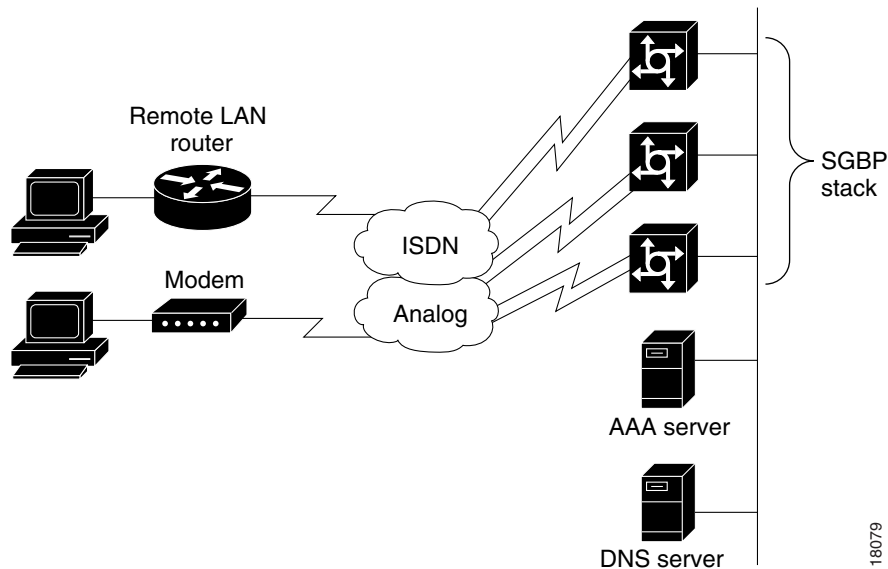
No MIBs or RFCs are supported by this feature.

## Functional Description

Large scale dialout enables scalable dialout 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 TACACS+ protocols. One or more network access servers can advertise summary routes to the remote destinations, then dynamically download the dialout profile configurations as needed.

Large scale dialout 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. 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 1 illustrates the large scale dialout solution.

Figure 1 Large Scale Dialout Components



Large scale dialout 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 alternative network access server. You can use any routing protocol that supports redistributing static and connected routes, and supports flash updates when a routing topology changes. The OSPF and EIGRP routing protocols are recommended.

## Next Hop Definition

A next hop address or remote name that you define is used in a AAA server lookup to retrieve the remote network's or host's user profile. 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 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 dialout 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 pointing 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 defining 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's 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.

## Configuration Tasks

The tasks to configure large scale dialout are described in the following sections:

- Establish the Route to the Remote Network
- Enable AAA and Static Route Download
- Enable Access to the AAA Server
- Enable Reverse DNS
- Enable SGBP Dialout Connection Bidding
- Define a User Profile
- Monitor and Maintain the Large Scale Dialout Network

See the examples in the section “Configuration Examples” for ideas on how you can implement large scale dialout in your network.

### Establish the Route to the Remote Network

This task 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) holding the user profile, use the **ip route** command in global configuration mode:

Command	Purpose
<b>ip route</b> <i>network-number</i> [ <i>network-mask</i> ] { <i>address</i>   <i>interface</i> } [ <i>distance</i> ] [ <b>name</b> <i>name</i> ]	Establish 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 remote network's AAA profile.

## Enable AAA and Static Route Download

AAA network security must be enabled before performing the tasks in this section. For more information about enabling AAA, refer to the “AAA Overview” chapter in the Cisco IOS Release 12.0 *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 dialout 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:

Step	Command	Purpose
1	<b>aaa new-model</b>	Enable the AAA server.
2	<b>aaa route download</b> <i>[time]</i>	Download static routes from the AAA server periodically using the router's hostname.
3	<b>aaa authorization configuration default</b> <b>[radius   tacacs+]</b>	Download configuration information from AAA server.

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

## Enable Access to the AAA Server

To configure the dialer interface to be able 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
<b>dialer aaa</b>	Allow the dialer to use the AAA server to locate profiles for dialing information.

## Enable Reverse DNS

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

Command	Purpose
<b>dialer dns</b>	Use reverse DNS to obtain the name of the remote network's user profile.

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 dialout and dial in profiles.

## Enable SGBP Dialout Connection Bidding

You must configure SGBP before performing the tasks in this section. The *Dial Solutions Configuration Guide* 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
<b>sgbp dial-bids</b>	Allow the stack group to bid for the dialout call.

Once the stack group has been configured and enabled for dialout 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:

Step	Command	Purpose
1	<b>dialer congestion-threshold</b> <i>links</i>	Force the dialer to search for another uncongested system in the stack group.
2	<b>dialer reserved links</b> { <i>dialin-link</i>   <i>dialout link</i> }	Reserve links for dial in and dialout.

Additional dialer interface configuration information and commands are found in the *Dial Solutions Configuration Guide* and the *Dial Solutions Command Reference* books.

## Define a User Profile

Attributes are used to define specific AAA elements in a user profile. Large scale dialout supports a subset of Ascend attribute-value (AV) pairs, RADIUS attributes, and a map class attribute providing outbound dialing services, as described in Table 1.

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. In cases where 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*, and the chapter “TACACS+ Attribute-Value Pairs” in the *Cisco IOS 12.0 Security Configuration Guide*.

For an example of a user profile using the supported attributes, see the section “Sample User Profile on an Ascend RADIUS Server for NAS1” later in this document.

**Note** In the following attributes, 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 1 Large Scale Dialout Outbound Service Attributes**

Number	Attribute	Description
<b>Ascend AV Pairs</b>		
#214	<b>Ascend-Send-Secret</b>	<p>Specifies the password the network access server uses when the remote site challenges the network access server to authenticate using either CHAP or PAP.</p> <p><b>Cisco AV Pair:</b> None</p> <p><b>TACACS+ Support:</b>  <pre>service = outbound {     send-secret = VALUE }</pre> </p> <p><b>Value:</b> Password string</p> <p><b>Note</b> The password is encrypted. This attribute requires a special RADIUS daemon that supports CHAP or PAP authentication.</p>
#227	<b>Ascend-Dial-Number</b>	<p>Defines the number to dial.</p> <p><b>Cisco AV Pair:</b>  <pre>cisco-avpair="outbound:dial-number=VALUE"</pre> </p> <p><b>TACACS+ Support:</b>  <pre>service = outbound {     dial-number = VALUE }</pre> </p> <p><b>Value:</b> Dial string</p> <p><b>Note</b> This attribute defines the plain dial number. It can be used in different profiles, whereas the callback-dialstring attribute is only for callbacks.</p>
#231	<b>Ascend-Send-Auth</b>	<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, 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><b>Cisco AV Pair:</b>  <pre>cisco-avpair="outbound:send-auth=VALUE"</pre> </p> <p><b>TACACS+ Support:</b>  <pre>service = outbound {     send-auth = none/pap/chap }</pre> </p> <p><b>Value:</b>  0: Send-Auth-None  1: Send-Auth-PAP  2: Send-Auth-CHAP</p>

**Table 1 Large Scale Dialout Outbound Service Attributes (Continued)**

Number	Attribute	Description
#247	Ascend-Data-SVC	<p>Specifies the type of data service the link uses for outgoing calls.</p> <p><b>Cisco AV Pair:</b>  <code>cisco-avpair="outbound:data-service=VALUE"</code></p> <p><b>TACACS+ Support:</b>  <pre>service = outbound {     data-service = VALUE }</pre></p> <p><b>Value:</b>                      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><b>Cisco AV Pair:</b>  <code>cisco-avpair="outbound:force-56=VALUE"</code></p> <p><b>TACACS+ Support:</b>  <pre>service = outbound {     force-56 = TRUE }</pre></p> <p><b>Value:</b>                      True: turns on this attribute (any other value is treated as false).</p>
<b>RADIUS (IETF) Attributes</b>		
#10	Framed-Routing	<p>Indicates a routing method when a router is used to access a network.</p> <p><b>Cisco AV Pair:</b>                      None</p> <p><b>TACACS+ Support:</b>  <pre>service = outbound {     routing = TRUE or FALSE }</pre></p> <p><b>Value:</b>                      True and false are the only valid values for both inbound and outbound dial (for example, routing=true).</p> <p><b>Note</b> 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><b>Cisco AV Pair:</b>  <code>cisco-avpir="outbound:callback-dialstring=VALUE"</code></p> <p><b>TACACS+ Support:</b>                      Equivalent to the existing callback-dialstring attribute.</p> <p><b>Value:</b>                      Dial string</p> <p><b>Note</b> This is an alternate way of setting a callback number using a standard RADIUS attribute.</p>

**Table 1 Large Scale Dialout Outbound Service Attributes (Continued)**

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

## Monitor and Maintain the Large Scale Dialout Network

Use any of the following EXEC commands to monitor and maintain a large scale dialout network:

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

# Configuration Examples

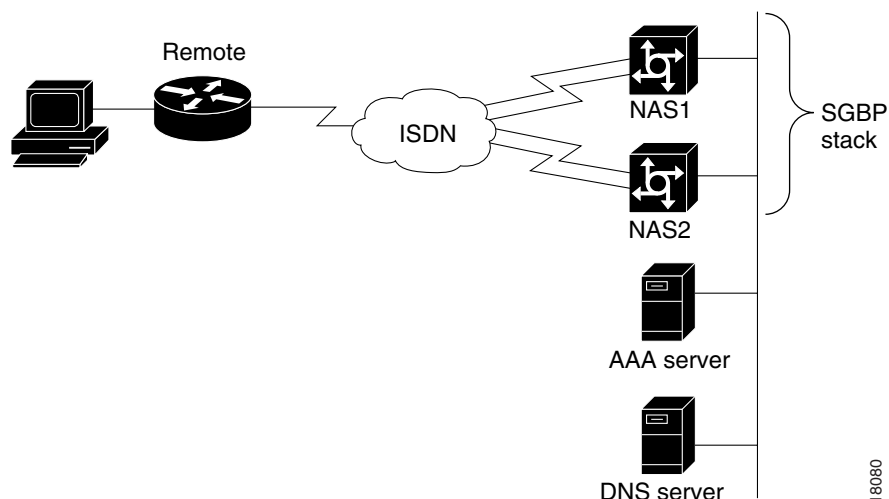
This section provides the following examples of how you can configure large scale dialout in your network:

- Stack Group and Static Route Download Configuration Example
- Sample User Profile on an Ascend RADIUS Server for NAS1
- Asynchronous Dialing Configuration Examples

## Stack Group and Static Route Download Configuration Example

In the following example, NAS1 will be configured as the primary network access server and NAS2 as the secondary network access server, in a stack group for dialout. The remote router is configured to answer calls. Figure 2 illustrates the configuration.

**Figure 2 Stack Group and Static Route Download Configuration**



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

A user profile for NAS1 on an Ascend RADIUS server is listed in the section “Sample User Profile on an Ascend RADIUS Server for NAS1.”

## Primary Network Access Server Configuration Example 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 Ethernet0
 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-Template1
 ip address 1.1.1.1 255.255.255.252
 no ip directed-broadcast
!
interface Virtual-Template2
 ip unnumbered Virtual-Template1
 no ip directed-broadcast
 ppp multilink
 multilink load-threshold 1 outbound
!
interface BRI0
 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 Dialer1
  ip unnumbered Ethernet0
  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 Example 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 Ethernet0
 ip address 172.21.17.17 255.255.255.0
 no ip directed-broadcast
 media-type 10BaseT
!
interface Virtual-Template1
 ip address 1.1.1.1 255.255.255.252
 no ip directed-broadcast
!
interface Virtual-Template2
 ip unnumbered Virtual-Template1
 no ip directed-broadcast
 ppp multilink
 multilink load-threshold 1 outbound
!
interface BRI0
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 dialer rotary-group 0
 isdn switch-type basic-5ess
 no fair-queue
!
interface Dialer0
 ip unnumbered Ethernet0
 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
```

## Router Remote Configuration Example

```

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 Loopback0
 ip address 172.31.229.41 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback1
 ip address 20.1.1.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback2
 ip address 20.1.2.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback3
 ip address 40.1.1.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0
 ip address 172.21.12.15 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface BRI0
 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 Dialer3
  ip unnumbered Loopback0
  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

```

## Sample User Profile on an Ascend RADIUS Server for NAS1

Following is an example of a dialout profile and a static route download profile in AAA. The dialout 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",
  cisco-avpair = "ip:route=20.1.1.0 255.255.255.0 172.31.229.41",
  cisco-avpair = "ip:route=20.1.2.0 255.255.255.0 172.31.229.41",
  cisco-avpair = "ip:route=20.1.3.0 255.255.255.0 172.31.229.41",
  cisco-avpair = "ip:route=40.1.1.0 255.255.255.0 172.31.229.41",

NAS1-1 Password = "cisco" User-Service-Type = Outbound-User,
  cisco-avpair = "ip:route=20.1.3.0 255.255.255.0 172.31.229.41 200",
  cisco-avpair = "ip:route=20.1.2.0 255.255.255.0 172.31.229.41 200",
  cisco-avpair = "ip:route=20.1.1.0 255.255.255.0 172.31.229.41 200",
  cisco-avpair = "ip:route=172.31.229.41 255.255.255.255 Dialer1 200 name
echo-8.cisco.com"

```

Static routes can also be defined using the Framed-Route IETF standard. The following shows how the above example for NAS1 would look using the Framed-Route IETF standard:

```

NAS1-1 Password = "cisco" User-Service-Type = Outbound-User,
  Framed-Route = "20.1.3.0/24 172.31.229.41.200",
  Framed-Route = "20.1.2.0/24 172.31.229.41.200",
  Framed-Route = "20.1.1.0/24 172.31.229.41.200",
  Framed-Route = "172.31.229.41/32 Dialer1 200 name echo-8.cisco.com"

```

## Asynchronous Dialing Configuration Examples

Large scale dialout supports dialing out using an asynchronous line. This 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 Configuration Example
- Asynchronous and Synchronous Dialing Configuration Example

### Asynchronous Dialing Configuration Example

The following is an example of an asynchronous dialing configuration.

```
chat-script dial "" "ATZ" OK "ATDT\T" TIMEOUT 60 CONNECT
!
interface Async1
 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 Dialer0
 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 Configuration Example

The following example creates a dialer rotary group for the asynchronous interfaces, and a dialer rotary group for the PRI interfaces. Any dialin or dialout reservations are applied only to the PRI dialer interface. In the configuration example below:

- Destinations that require modem calls have static routes pointing to Dialer0.
- Destinations requiring digital connections have static routes pointing to Dialer1.
- 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 Serial0:23
 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 Async1
 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 Dialer0
 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 Dialer1
 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
```

## Command Reference

This section documents new or modified commands required to configure the large scale dialout feature. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- **aaa authorization configuration default**
- **aaa route download**
- **clear dialer sessions**
- **clear ip route download**
- **dialer aaa**
- **dialer congestion-threshold**
- **dialer dns**
- **dialer reserved-links**
- **ip route**
- **sgbp dial-bids**
- **show dialer sessions**
- **show ip route**

## aaa authorization configuration default

To download static route configuration information from the AAA server using TACACS+ or RADIUS, use the **aaa authorization configuration default** command in global configuration mode. To remove static route configuration information, use the **no** form of this command.

```
aaa authorization configuration default {radius | tacacs+}  
no aaa authorization configuration default
```

### Syntax Description

<b>radius</b>	Use RADIUS for static route download.
<b>tacacs+</b>	Use TACACS+ for static route download.

### Default

No configuration authorization is defined.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

### Example

The following example downloads static route information using a TACACS+ server:

```
router(config)# aaa authorization configuration default tacacs+
```

### Related Commands

```
aaa new-model  
aaa route download  
clear ip route download  
show ip route
```

## aaa route download

To enable the download static route feature and set the amount of time between downloads, use the **aaa route download** command in global configuration mode. To disable this function, use the **no** form of the command.

```
aaa route download [time]  
no aaa route download
```

### Syntax Description

*time* (Optional) Time between downloads, in minutes. The range is 1 to 1440 minutes.

### Default

The default period between downloads (updates) is 720 minutes.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

This command is used to download static route details from the AAA server if the name of the router is *hostname*. The name passed to the AAA server for static routes is *hostname-1*, *hostname-2* .... *hostname-n* — the router downloads static routes until it fails an index and no more routes can be downloaded.

### Example

The following example sets the AAA route update period to 100 minutes:

```
router(config)# aaa route download 100
```

### Related Commands

```
aaa authorization configuration default  
clear ip route download  
show ip route
```

## clear dialer sessions

To remove all dialer sessions and disconnect links when connected, use the **clear dialer sessions** command in EXEC configuration mode.

**clear dialer sessions**

### Syntax Description

This command has no arguments or keywords.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

### Example

The following example of how to enter the **clear dialer sessions** command:

```
router# clear dialer sessions
```

### Related Commands

**show dialer sessions**

## clear ip route download

To clear static routes downloaded from a AAA server, use the **clear ip route download** command in EXEC configuration mode.

**clear ip route download** { \* | *network-number network-mask* | **reload** }

### Syntax Description

<b>*</b>	Deletes all routes.
<i>network-number network-mask</i>	Deletes only the destination network route; indicate the value in standard IP address notation. Example: 1.1.1.1 255.255.255.255.
<b>reload</b>	Deletes all routes, then reloads static routes from the AAA server and resets the timer configured by the <b>aaa route download</b> command.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

This command forces the router to reload static routes from the AAA server before the update timer expires.

### Example

The following example shows how to clear all routes:

```
router# clear ip route download *
```

### Related Commands

**aaa authorization configuration default**  
**aaa route download**  
**show ip route**

## dialer aaa

To allow a dialer to access the AAA server for dialing information, use the **dialer aaa** command in interface configuration mode. To disable this function, use the **no** form of the command.

**dialer aaa**  
**no dialer aaa**

### Syntax Description

This command has no arguments or keywords.

### Default

This feature is not enabled by default.

### Command Mode

Interface configuration of a dialer rotary group leader.

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

This command is required for large scale dialout functionality. See the section “Define a User Profile” for information about defining AAA elements in a user profile.

### Example

The following example shows how to allow a dialer interface access to the AAA server for dialing information:

```
router(config)# interface Dialer0  
router(config-if)# dialer aaa
```

### Related Commands

**dialer congestion-threshold**

## dialer congestion-threshold

To specify congestion threshold in connected links, use the **dialer congestion-threshold** command in interface configuration mode. To disable this function, use the **no** form of the command.

**dialer congestion-threshold** *links*  
**no dialer congestion-threshold**

### Syntax Description

*links*      Number of connected links for congestion threshold in the range 0 to 64000.

### Default

The default number of connected links is 64000.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

This command is used to force the dialer to search for another uncongested system (the alternate network access server) in a stack group to dial out using SGBP.

### Example

The following example sets the congestion threshold to five connected links on the Dialer 0 interface:

```
router(config)# interface Dialer0  
router(config-if)# dialer aaa  
router(config-if)# dialer congestion-threshold 5
```

### Related Commands

**dialer reserved-links**  
**sgbp dial-bids**

## dialer dns

To obtain a user profile name on a remote network using reverse DNS, use the **dialer dns** command in interface configuration mode. Use the **no** form of this command to disable this function.

**dialer dns**  
**no dialer dns**

### Syntax Description

This command has no arguments or keywords.

### Default

The reverse DNS function is disabled by default.

### Command Mode

Interface configuration of a dialer rotary group leader.

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

This command allows the dialer to use reverse DNS to get a profile name for accessing the AAA server. This command is not required when using named static routes.

### Example

The following example shows how to allow the dialer to use reverse DNS for name lookup:

```
router(config)# interface Dialer0  
router(config-if)# dialer aaa  
router(config-if)# dialer dns
```

### Related Commands

**dialer aaa**

## dialer reserved-links

To reserve links for dial in and dialout, use the **dialer reserved-links** command in interface configuration mode.

**dialer reserved links** {*dialin-link* \ *dialout link*}  
**no dialer reserved links**

### Syntax Description

<i>dialin-link</i>	Link reserved for dial in.
<i>dialout-link</i>	Link reserved for dialout.

### Default

By default, no links are reserved.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

### Example

The following example sets dial in reserved links to 1 and dialout reserved links to 0 on the Dialer0 interface:

```
router(config)# interface Dialer0  
router(config-if)# dialer aaa  
router(config-if)# dialer reserved-links 1 0
```

### Related Commands

**dialer congestion-threshold**  
**sgbp dial-bids**

## ip route

To establish static routes and define the next hop for large scale dialout, use the **ip route** command in global configuration mode. To remove static routes, use the **no ip route** command.

```
ip route network-number network-mask {IP address | interface} [distance] [name name]  
no ip route
```

### Syntax Description

<i>network-number</i>	IP address of the target network or subnet.
<i>network-mask</i>	Network mask that lets you mask network and subnetwork bits.
<i>IP address</i>	Internet address of the next hop that can be used to reach that network in standard IP address notation. Example: 1.1.1.1.
<i>interface</i>	Network interface to use.
<i>distance</i>	(Optional) An administrative distance, which is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers.
<b>name</b> <i>name</i>	(Optional) Name of the user profile.

### Default

No static route is established.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

A static route is appropriate when the communication server cannot dynamically build a route to the destination.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, IGRP-derived routes have a default administrative distance of 100. To have a static route that would be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface will be advertised using RIP, IGRP, and other dynamic routing protocols, regardless of whether redistribute static commands were specified for those routing protocols. These static routes will be advertised because static routes that point to an interface are considered to be connected in the routing table and hence lose their static nature. However, if you define a static route to an interface that is not in one of the networks defined in a network command, no dynamic routing protocols will advertise the route unless a redistribute static command is specified for these protocols.

The user profile name is passed to an AAA server as the next hop for large scale dialout, and is the *name* argument with the -out suffix appended. The suffix is automatically supplied and is required since dial in and user profile names must be unique.

### Example

In the following example, an administrative distance of 110 was chosen. In this case, packets for network 10.0.0.0 will be routed via to the communication server at 172.19.3.4 if dynamic information with administrative distance less than 110 is not available:

```
router(config)# ip route 10.0.0.0 255.0.0.0 172.19.3.4 110
```

In the following example, packets for network 172.19.0.0 will be routed to the communication server at 172.19.6.6:

```
router(config)# ip route 172.19.0.0 255.255.0.0 172.19.6.6
```

In the following example, the user profile named macarthur-out will be retrieved from the AAA:

```
router(config)# ip route 10.0.0.0 255.255.255.255 Dialer0 name macarthur
```

### Related Commands

**show ip route**

## sgbp dial-bids

To allow the stack group to bid for dialout connection, use the **sgbp dial-bids** command in global configuration mode. To disable this function, use the **no** form of this command.

```
sgbp dial-bids  
no sgbp dial-bids
```

### Syntax Description

This command has no arguments or keywords.

### Default

The stack group bid function is disabled by default.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

### Example

The following example shows how to configure a stack group for large scale dialout:

```
router(config)# sgbp group forever  
router(config)# sgbp member NAS2 172.21.17.17  
router(config)# sgbp dial-bids
```

### Related Commands

```
dialer congestion-threshold  
dialer reserved-links  
sgbp group  
sgbp member
```

## show dialer sessions

To display all dialer sessions, use the **show dialer sessions** command in EXEC configuration mode.

**show dialer sessions**

### Syntax Description

This command has no arguments or keywords.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

### Example

In the following example, a Cisco 5300 router is dialing out to a Cisco 5200 router. All dialer sessions are displayed:

```
router# show dialer sessions

DSES 0xAF0: index = 0x0, state = 3, ip addr = 11.2.2.22, dialed number = 81067, name = p5
200_pri.cisco.com, connected interface = Serial0:22
```

Table 2 describes the fields seen in this display.

**Table 2 Show Dialer Sessions Field Descriptions**

Field	Description
ip addr	IP address of the remote interface that has been dialed into.
dialed number	Number that was used to dial out.
name	Name of the interface dialed into. This can be different from the router name, as names can be changed on per-interface basis.
connected interface	The channel on which the call is connected.

### Related Commands

**clear dialer sessions**

## show ip route

To display all static IP routes, or those installed using the AAA route download function, use the **show ip route EXEC** command.

```
show ip route [address [network-mask] [longer-prefixes]] | [protocol [process-id]] |
[static [download]]
```

### Syntax Description

<i>address</i>	(Optional) The IP address about which routing information should be displayed.
<i>network-mask</i>	(Optional) Network mask that lets you mask network and subnetwork bits.
<b>longer-prefixes</b>	(Optional) The <i>address</i> and <i>mask</i> pair becomes a prefix, and any routes that match that prefix are displayed.
<i>protocol</i>	(Optional) Name of a routing protocol; or the keyword <b>connected</b> , <b>static</b> , or <b>summary</b> . If you specify a routing protocol, use one of the following keywords: <b>bgp</b> , <b>egp</b> , <b>eigrp</b> , <b>hello</b> , <b>igrp</b> , <b>isis</b> , <b>ospf</b> , or <b>rip</b> .
<i>process-id</i>	(Optional) Arbitrary number assigned to identify a process of the specified protocol.
<b>static</b>	(Optional) All static routes.
<b>download</b>	(Optional) The route installed using the AAA route download function.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **longer-prefixes** keyword first appeared in Cisco IOS Release 11.0. The *process-id* argument first appeared in Cisco IOS Release 10.3. The **static** and **download** keywords first appeared in Cisco IOS Release 12.0(3)T.

The **show ip route static download** command provides a way to display all dynamic static routes with name and distance information, including active and inactive ones. You can display all active dynamic static routes with both the **show ip route** and **show ip route static** commands after these active routes are added in the main routing table.

### Examples

The following examples display all downloaded static routes. A P designates which route was installed using AAA route download.

```
router# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route
```

```
Gateway of last resort is 172.21.17.1 to network 0.0.0.0

      172.31.0.0/32 is subnetted, 1 subnets
P      172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3
subnets
P      20.1.1.0 [200/0] via 172.31.229.41, Dialer1
P      20.1.3.0 [200/0] via 172.31.229.41, Dialer1
P      20.1.2.0 [200/0] via 172.31.229.41, Dialer1

router# show ip route static

      103.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
P      103.1.1.1/32 is directly connected, BRI0
P      103.0.0.0/8 [1/0] via 103.1.1.1, BRI0
S      172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S      18.0.0.0/8 is directly connected, BRI0
P      20.0.0.0/8 is directly connected, BRI0
      172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S      172.21.114.201/32 is directly connected, BRI0
S      172.21.114.205/32 is directly connected, BRI0
S      172.21.114.174/32 is directly connected, BRI0
S      172.21.114.12/32 is directly connected, BRI0
P      10.0.0.0/8 is directly connected, BRI0
P      11.0.0.0/8 is directly connected, BRI0
P      12.0.0.0/8 is directly connected, BRI0
S*     0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
S      198.92.0.0/16 [1/0] via 172.21.114.65, Ethernet0
```

The following example shows how to use the **show ip route static download** command to see all active and inactive routes installed using the AAA route download feature:

```
router# show ip route static download

Connectivity: A - Active, I - Inactive

A      10.0.0.0 255.0.0.0 BRI0
A      11.0.0.0 255.0.0.0 BRI0
A      12.0.0.0 255.0.0.0 BRI0
A      20.0.0.0 255.0.0.0 BRI0
I      21.0.0.0 255.0.0.0 172.21.1.1
I      22.0.0.0 255.0.0.0 Serial0
I      30.0.0.0 255.0.0.0 Serial0
I      31.0.0.0 255.0.0.0 Serial1
I      32.0.0.0 255.0.0.0 Serial1
A      103.0.0.0 255.0.0.0 103.1.1.1
A      103.1.1.1 255.255.255.255 BRI0 200 name remotel
I      104.21.69.0 255.255.255.0 104.21.69.1
```

## Related Commands

**show dialer interface**

## Debug Commands

The following is a new **debug** command for the large scale dialout feature:

- **debug sgbp dial-bids**

The following are related **debug** commands for large scale dialout. You can find descriptions of their use in the Cisco IOS *Debug Command Reference*, or by using the master index, or by searching online.

- **debug radius**
- **debug tacacs+**
- **debug aaa authorization**
- **debug aaa authentication**
- **debug dialer events**
- **debug ppp authentication**

## debug sgbp dial-bids

To display large scale dialout negotiations between the primary network access server and alternate network access servers, use the **debug sgbp dial-bids** EXEC command. The **no** form of this command disables debugging output.

**[no] debug sgbp dial-bids**

### Usage Guidelines

Use this command only when the **sgbp dial-bids** command has been configured.

### Sample Displays

The following is sample output from the **debug sgbp dial-bids** command:

```
router# debug sgbp dial-bids

*Jan 1 00:25:03.643: SGBP-RES: New bid add request: 4B0 8 2 1 DAC0 1 1
This indicates a new dialout bid has started.
*Jan 1 00:25:03.643: SGBP-RES: Sent Discover message to ID 7B09B71E 49 bytes
The bid request has been sent.
*Jan 1 00:25:03.647: SGBP-RES: Received Message of 49 length:

*Jan 1 00:25:03.647: SGBP-RES: header 5 30 0 31
2 0 0 2D 0 0 0 0 0 0 0 3 0 0 0 1 1E AF 3A 41 7B 9 B7 1E 8 15
B 3 2 C 6 0 0 DA C0 D 4 0 0 E 3 1 F 3 1
*Jan 1 00:25:03.647:
*Jan 1 00:25:03.647: SGBP RES: Scan: Message type: Offer
*Jan 1 00:25:03.647: SGBP RES: Scan: Len is 45
*Jan 1 00:25:03.647: SGBP RES: Scan: Transaction ID: 3
*Jan 1 00:25:03.647: SGBP RES: Scan: Message ID: 1
*Jan 1 00:25:03.647: SGBP RES: Scan: Client ID: 1EAF3A41
*Jan 1 00:25:03.651: SGBP RES: Scan: Server ID: 7B09B71E
*Jan 1 00:25:03.651: SGBP RES: Scan: Resource type 8 length 21
*Jan 1 00:25:03.651: SGBP RES: Scan: Phy-Port Media type: ISDN
*Jan 1 00:25:03.651: SGBP RES: Scan: Phy-Port Min BW: 56000
*Jan 1 00:25:03.651: SGBP RES: Scan: Phy-Port Num Links: 0
*Jan 1 00:25:03.651: SGBP RES: Scan: Phy-Port User class: 1
*Jan 1 00:25:03.651: SGBP RES: Scan: Phy-Port Priority: 1
*Jan 1 00:25:03.651: SGBP-RES: received 45 length Offer packet
*Jan 1 00:25:03.651: SGBP-RES: Offer from 7B09B71E for Transaction 3 accepted
*Jan 1 00:25:03.651: SGBP RES: Server is uncongested. Immediate win
An alternate network access server has responded and won the bid.
*Jan 1 00:25:03.651: SGBP-RES: Bid Succeeded handle 7B09B71E Server-id 4B0
*Jan 1 00:25:03.651: SGBP-RES: Sent Dial-Req message to ID 7B09B71E 66 bytes
The primary network access server has asked the alternate server to dial.
*Jan 1 00:25:04.651: SGBP-RES: QScan: Purging entry
*Jan 1 00:25:04.651: SGBP-RES: deleting entry 6112E204 1EAF3A41 from list...
```