



Configuring Multiprotocol BGP (MP-BGP) Support for CLNS

First Published: February 28, 2007

Last Updated: February 28, 2007

This module describes configuration tasks to configure multiprotocol BGP (MP-BGP) support for CLNS, which provides the ability to scale Connectionless Network Service (CLNS) networks. The multiprotocol extensions of Border Gateway Protocol (BGP) add the ability to interconnect separate Open System Interconnection (OSI) routing domains without merging the routing domains, thus providing the capability to build very large OSI networks.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Configuring MP-BGP Support for CLNS” section on page 36](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for Configuring MP-BGP Support for CLNS, page 2](#)
- [Information About Configuring MP-BGP Support for CLNS, page 2](#)
- [How to Configure MP-BGP Support for CLNS, page 6](#)
- [Configuration Examples for MP-BGP Support for CLNS, page 26](#)
- [Additional References, page 35](#)
- [Feature Information for Configuring MP-BGP Support for CLNS, page 36](#)
- [Glossary, page 38](#)



Restrictions for Configuring MP-BGP Support for CLNS

The configuration of MP-BGP support for CLNS does not support the creation and use of BGP confederations within the CLNS network. We recommend the use of route reflectors to address the issue of a large internal BGP mesh.

BGP extended communities are not supported by this feature.

The following BGP commands are not supported by this feature:

- **auto-summary**
- **neighbor advertise-map**
- **neighbor distribute-list**
- **neighbor soft-reconfiguration**
- **neighbor unsuppress-map**

Information About Configuring MP-BGP Support for CLNS

To configure the MP-BGP support for CLNS, you should understand the following concepts:

- [Design Features of MP-BGP Support for CLNS, page 2](#)
- [Generic BGP CLNS Network Topology, page 3](#)
- [DCN Network Topology, page 4](#)
- [Benefits of MP-BGP Support for CLNS, page 6](#)

Design Features of MP-BGP Support for CLNS

The configuration of MP-BGP support for CLNS allows Border Gateway Protocol (BGP) to be used as an interdomain routing protocol in networks that use Connectionless Network Service (CLNS) as the network-layer protocol. This feature was developed to solve a scaling issue with a data communications network (DCN) where large numbers of network elements are managed remotely. For details about the DCN issues and how to implement this feature in a DCN topology, see the “[DCN Network Topology](#)” [section on page 4](#).”

BGP, as an Exterior Gateway Protocol, was designed to handle the volume of routing information generated by the Internet. Network administrators can control the BGP routing information because BGP neighbor relationships (peering) are manually configured and routing updates use incremental broadcasts. Some interior routing protocols such as Intermediate System-to-Intermediate System (IS-IS), in contrast, use a form of automatic neighbor discovery technique and broadcast updates at regular intervals.

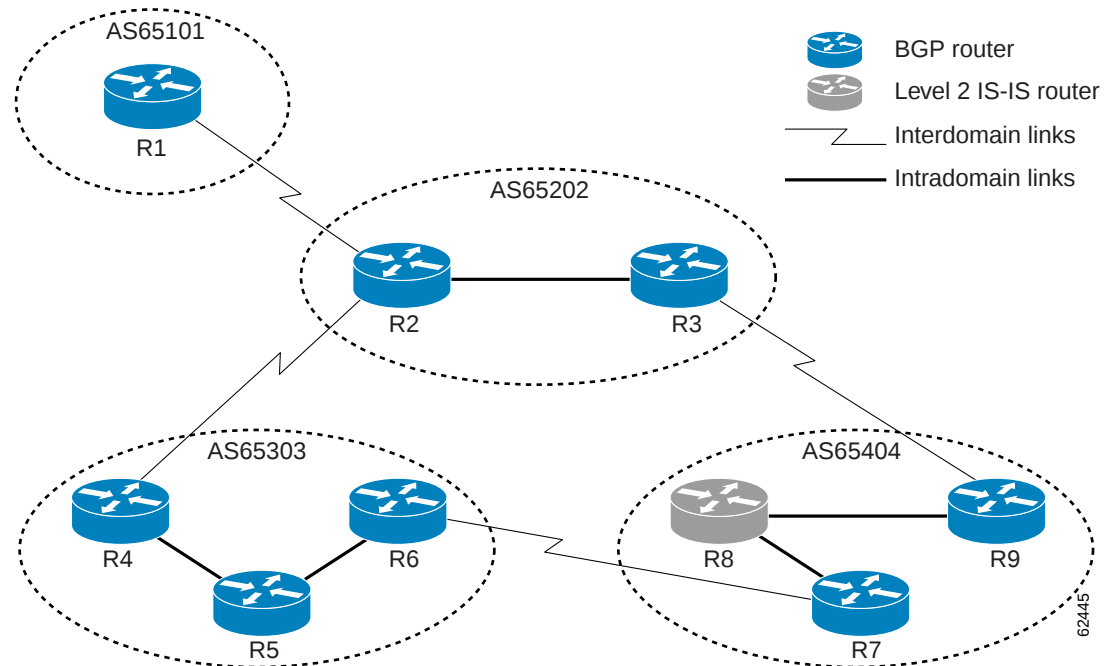
CLNS uses network service access point (NSAP) addresses to identify all its network elements. Using the BGP address-family support, NSAP address prefixes can be transported using BGP. In CLNS, BGP prefixes are inserted into the CLNS Level 2 prefix table. This functionality allows BGP to be used as an interdomain routing protocol between separate CLNS routing domains.

Implementing BGP in routers at the edge of each internal network means that the existing interior protocols need not be changed, minimizing disruption in the network.

Generic BGP CLNS Network Topology

Figure 1 shows a generic BGP CLNS network containing nine routers that are grouped into four different autonomous systems (in BGP terminology) or routing domains (in OSI terminology). To avoid confusion, in this document we will use the BGP terminology of autonomous systems because each autonomous system is numbered and therefore more easily identified in the diagram and in the configuration discussion.

Figure 1 Components in a Generic BGP CLNS Network



Within each autonomous system, IS-IS is used as the intradomain routing protocol. Between autonomous systems, BGP and its multiprotocol extensions are used as the interdomain routing protocol. Each router is running either a BGP or Level 2 IS-IS routing process. To facilitate this feature, the BGP routers are also running a Level 2 IS-IS process. Although the links are not shown in the figure, each Level 2 IS-IS router is connected to multiple Level 1 IS-IS routers that are, in turn, connected to multiple CLNS networks.

Each autonomous system in this example is configured to demonstrate various BGP features and how these features work with CLNS to provide a scalable interdomain routing solution. In [Figure 1 on page 3](#), the autonomous system AS65101 has a single Level 2 IS-IS router, R1, and is connected to just one other autonomous system, AS65202. Connectivity to the rest of the network is provided by R2, and a default route is generated for R1 to send to R2 all packets with destination NSAP addresses outside of AS65101.

In AS65202 there are two routers, R2 and R3, both with different external BGP (eBGP) neighbors. Routers R2 and R3 are configured to run internal BGP (iBGP) over the internal connection between them.

AS65303 shows how the use of BGP peer groups and route reflection can minimize the need for TCP connections between routers. Fewer connections between routers simplifies the network design and the amount of traffic in the network.

AS65404 shows how to use redistribution to communicate network reachability information to a Level 2 IS-IS router that is not running BGP.

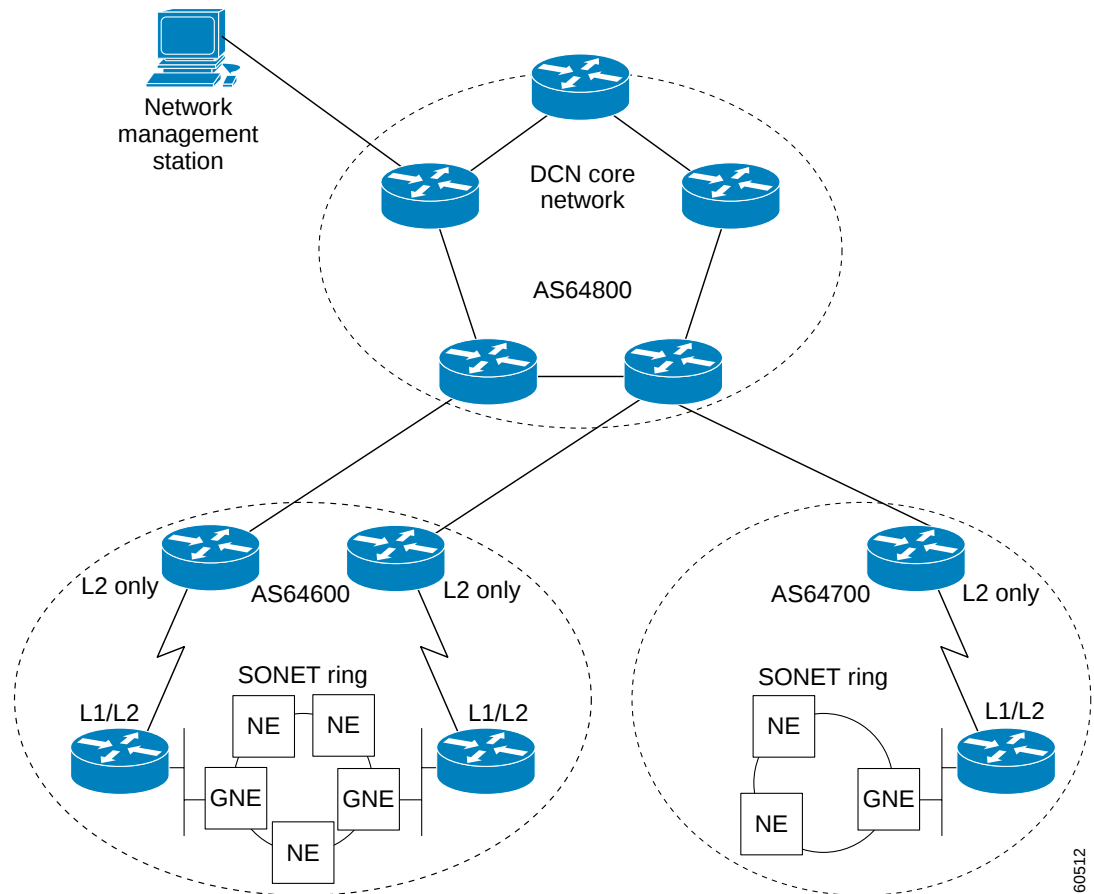
The configuration tasks and examples in this document are based on the generic network design shown in [Figure 1 on page 3](#). Configurations for all the routers in [Figure 1](#) are listed in the “[Implementing MP-BGP Support for CLNS: Example](#)” section on page 30.

DCN Network Topology

The Multiprotocol BGP (MP-BGP) Support for CLNS feature can benefit a data communications network (DCN) managing a large number of remote SONET rings. SONET is typically used by telecommunications companies to send data over fiber-optic networks.

[Figure 2](#) shows some components of a DCN network. To be consistent with the BGP terminology, the figure contains labels to indicate three autonomous systems instead of routing domains. The network elements—designated by NE in [Figure 2](#)—of a SONET ring are managed by OSI protocols such as File Transfer, Access, and Management (FTAM) and Common Management Information Protocol (CMIP). FTAM and CMIP run over the CLNS network-layer protocol, which means that the routers providing connectivity must run an OSI routing protocol.

Figure 2 Components in a DCN Network



IS-IS is a link-state protocol used in this example to route CLNS. Each routing node (networking device) is called an intermediate system (IS). The network is divided into areas defined as a collection of routing nodes. Routing within an area is referred to as Level 1 routing. Routing between areas involves Level 2 routing. Routers that link a Level 1 area with a Level 2 area are defined as Level 1-2 routers. A network element that connects to the Level 2 routers that provide a path to the DCN core is represented by a gateway network element—GNE in Figure 2. The network topology here is a point-to-point link between each network element router. In this example, a Level 1 IS-IS router is called an NE router.

Smaller Cisco routers such as the Cisco 2600 series were selected to run as the Level 1-2 routers because shelf space in the central office (CO) of a service provider is very expensive. A Cisco 2600 series router has limited processing power if it is acting as the Level 1 router for four or five different Level 1 areas. The number of Level 1 areas under this configuration is limited to about 200. The entire Level 2 network is also limited by the speed of the slowest Level 2 router.

To provide connectivity between NE routers, in-band signaling is used. The in-band signaling is carried in the SONET/Synchronous Digital Hierarchy (SDH) frame on the data communications channel (DCC). The DCC is a 192-KB channel, which is a very limited amount of bandwidth for the management traffic. Due to the limited signaling bandwidth between network elements and the limited amount of processing power and memory in the NE routers running IS-IS, each area is restricted to a maximum number of 30 to 40 routers. On average, each SONET ring consists of 10 to 15 network elements.

With a maximum of 200 areas containing 10 to 15 network elements per area, the total number of network element routers in a single autonomous system must be fewer than 3000. Service providers are looking to implement over 10,000 network elements as their networks grow, but the potential number of network elements in an area is limited. The current solution is to break down the DCN into a number of smaller autonomous systems and connect them using static routes or ISO Interior Gateway Routing Protocol (IGRP). ISO IGRP is a proprietary protocol that can limit future equipment implementation options. Static routing does not scale because the growth in the network can exceed the ability of a network administrator to maintain the static routes. BGP has been shown to scale to over 100,000 routes.

To implement the Multiprotocol BGP (MP-BGP) Support for CLNS feature in this example, configure BGP to run on each router in the DCN core network—AS64800 in Figure 2—to exchange routing information between all the autonomous systems. In the autonomous systems AS64600 and AS64700, only the Level 2 routers will run BGP. BGP uses TCP to communicate with BGP-speaking neighbor routers, which means that both an IP-addressed network and an NSAP-addressed network must be configured to cover all the Level 2 IS-IS routers in the autonomous systems AS64600 and AS64700 and all the routers in the DCN core network.

Assuming that each autonomous system—for example, AS64600 and AS64700 in Figure 2—remains the same size with up to 3000 nodes, we can demonstrate how large DCN networks can be supported with this feature. Each autonomous system advertises one address prefix to the core autonomous system. Each address prefix can have two paths associated with it to provide redundancy because there are two links between each autonomous system and the core autonomous system. BGP has been shown to support 100,000 routes, so the core autonomous system can support many other directly linked autonomous systems because each autonomous system generates only a few routes. We can assume that the core autonomous system can support about 2000 directly linked autonomous systems. With the hub-and-spoke design where each autonomous system is directly linked to the core autonomous system, and not acting as a transit autonomous system, the core autonomous system can generate a default route to each linked autonomous system. Using the default routes, the Level 2 routers in the linked autonomous systems process only a small amount of additional routing information. Multiplying the 2000 linked autonomous systems by the 3000 nodes within each autonomous system could allow up to 6 million network elements.

Benefits of MP-BGP Support for CLNS

The Multiprotocol BGP (MP-BGP) Support for CLNS feature adds the ability to interconnect separate OSI routing domains without merging the routing domains, which provides the capability to build very large OSI networks. The benefits of using this feature are not confined to DCN networks, and can be implemented to help scale any network using OSI routing protocols with CLNS.

How to Configure MP-BGP Support for CLNS

This section contains the following procedures. It may not be necessary to go through each procedure for your particular network. You must perform the steps in the required procedures, but all other procedures are done as required for your network.

- [Configuring and Activating a BGP Neighbor to Support CLNS, page 6](#) (required)
- [Configuring an IS-IS Routing Process, page 8](#) (required)
- [Configuring Interfaces That Connect to BGP Neighbors, page 9](#) (required)
- [Configuring Interfaces Connected to the Local OSI Routing Domain, page 11](#) (required)
- [Advertising Networking Prefixes, page 12](#) (as required)
- [Redistributing Routes from BGP into IS-IS, page 14](#) (as required))
- [Redistributing Routes from IS-IS into BGP, page 15](#) (as required)
- [Configuring BGP Peer Groups and Route Reflectors, page 16](#)
- [Filtering Inbound Routes Based on NSAP Prefixes, page 18](#) (as required)
- [Filtering Outbound BGP Updates Based on NSAP Prefixes, page 19](#) (as required)
- [Originating Default Routes for a Neighboring Routing Domain, page 21](#) (as required)
- [Verifying MP-BGP Support for CLNS, page 22](#) (as required)
- [Troubleshooting MP-BGP Support for CLNS, page 24](#) (as required)

Configuring and Activating a BGP Neighbor to Support CLNS

To configure and activate a BGP routing process and an associated BGP neighbor (peer) to support CLNS, perform the steps in this procedure.

Address Family Routing Information

By default, commands entered under **router bgp** command apply to the IPv4 address family. This will continue to be the case unless you enter the **no bgp default ipv4-unicast** command as the first command under the **router bgp** command. The **no bgp default ipv4-unicast** command is configured on the router to disable the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **address-family nsap** [**unicast**]
7. **neighbor** *ip-address* **activate**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router bgp <i>as-number</i> Example: Router(config)# router bgp 65101	Configures a BGP routing process and enters router configuration mode. The <i>as-number</i> argument identifies the autonomous system in which the router resides. Valid values are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.
Step 4	no bgp default ipv4-unicast Example: Router(config-router)# no bgp default ipv4-unicast	Disables the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers.
Step 5	neighbor { <i>ip-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i> Example: Router(config-router)# neighbor 10.1.2.2 remote-as 64202	Adds an IP address or peer group name of the BGP neighbor in the specified autonomous system to the BGP neighbor table of the local router.
Step 6	address-family nsap [unicast] Example: Router(config-router)# address-family nsap	Specifies the NSAP address family and enters address family configuration mode. The optional unicast keyword specifies the NSAP unicast address prefixes. By default, the router is placed in configuration mode for the unicast NSAP address family if the unicast keyword is not specified with the address-family nsap command.

	Command or Action	Purpose
Step 7	neighbor ip-address activate	Enables the BGP neighbor to exchange prefixes for the NSAP address family with the local router.
	Example: Router(config-router-af)# neighbor 10.1.2.2 activate	Note If you have configured a peer group as a BGP neighbor, you do not use this command because peer groups are automatically activated when any peer group parameter is configured.
Step 8	end	Exits address family configuration mode and returns to privileged EXEC mode.
	Example: Router(config-router-af)# end	

Configuring an IS-IS Routing Process

When an integrated IS-IS routing process is configured, the first instance of the IS-IS routing process configured is by default a Level 1-2 (intra-area and interarea) router. All subsequent IS-IS routing processes on a network running CLNS are configured as Level 1. All subsequent IS-IS routing processes on a network running IP are configured as Level-1-2. To use the Multiprotocol BGP (MP-BGP) Support for CLNS feature, configure a Level 2 routing process.

To configure an IS-IS routing process and assign it as a Level-2-only process, perform the steps in this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis area-tag**
4. **net network-entity-title**
5. **is-type [level-1 | level-1-2 | level-2-only]**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	• Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	<pre>router isis area-tag</pre> Example: Router(config)# router isis osi-as-101	Configures an IS-IS routing process and enters router configuration mode for the specified routing process. The <i>area-tag</i> argument is a meaningful name for a routing process. It must be unique among all IP and CLNS routing processes for a given router.
Step 4	<pre>net network-entity-title</pre> Example: Router(config-router)# net 49.0101.1111.1111.1111.1111.00	Configures a network entity title (NET) for the routing process. If you are configuring multiarea IS-IS, you must specify a NET for each routing process.
Step 5	<pre>is-type [level-1 level-1-2 level-2-only]</pre> Example: Router(config-router)# is-type level-1	Configures the router to act as a Level 1 (intra-area) router, as both a Level 1 router and a Level 2 (interarea) router, or as an interarea router only. In multiarea IS-IS configurations, the first instance of the IS-IS routing process configured is by default a Level 1-2 (intra-area and interarea) router. All subsequent IS-IS routing processes on a network running CLNS are configured as Level 1. All subsequent IS-IS routing processes on a network running IP are configured as Level-1-2.
Step 6	<pre>end</pre> Example: Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

Configuring Interfaces That Connect to BGP Neighbors

When a router running IS-IS is directly connected to an eBGP neighbor, the interface between the two eBGP neighbors is activated using the **clns enable** command, which allows CLNS packets to be forwarded across the interface. The **clns enable** command activates the End System-to-Intermediate System (ES-IS) protocol to search for neighboring OSI systems.



Note

Running IS-IS across the same interface that is connected to an eBGP neighbor can lead to undesirable results if the two OSI routing domains merge into a single domain.

When a neighboring OSI system is found, BGP checks that it is also an eBGP neighbor configured for the NSAP address family. If both the preceding conditions are met, BGP creates a special BGP neighbor route in the CLNS Level 2 prefix routing table. The special BGP neighbor route is automatically redistributed in to the Level 2 routing updates so that all other Level 2 IS-IS routers in the local OSI routing domain know how to reach this eBGP neighbor.

To configure interfaces that are being used to connect with eBGP neighbors, perform the steps in this procedure. These interfaces will normally be directly connected to their eBGP neighbor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **clns enable**
6. **no shutdown**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface serial 2/0	Specifies the interface type and number and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> Example: Router(config-if)# ip address 10.1.2.2 255.255.255.0	Configures the interface with an IP address.
Step 5	clns enable Example: Router(config-if)# clns enable	Specifies that CLNS packets can be forwarded across this interface. The ES-IS protocol is activated and starts to search for adjacent OSI systems.
Step 6	no shutdown Example: Router(config-if)# no shutdown	Turns on the interface.
Step 7	end Example: Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Interfaces Connected to the Local OSI Routing Domain

To configure interfaces that are connected to the local OSI routing domain, perform the steps in this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **clns router isis** *area-tag*
6. **ip router isis** *area-tag*
7. **no shutdown**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface ethernet 0/1	Specifies the interface type and number and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> Example: Router(config-if)# ip address 10.2.3.1 255.255.255.0	Configures the interface with an IP address. Note This step is required only when the interface needs to communicate with an iBGP neighbor.
Step 5	clns router isis <i>area-tag</i> Example: Router(config-if)# clns router isis osi-as-202	Specifies that the interface is actively routing IS-IS when the network protocol is ISO CLNS and identifies the area associated with this routing process.

	Command or Action	Purpose
Step 6	<code>ip router isis area-tag</code>	Specifies that the interface is actively routing IS-IS when the network protocol is IP and identifies the area associated with this routing process.
	Example: Router(config-if)# ip router isis osi-as-202	Note This step is required only when the interface needs to communicate with an iBGP neighbor, and the IGP is IS-IS.
Step 7	<code>no shutdown</code>	Turns on the interface.
	Example: Router(config-if)# no shutdown	
Step 8	<code>end</code>	Exits interface configuration mode and returns to privileged EXEC mode.
	Example: Router(config-if)# end	

Advertising Networking Prefixes

Advertising NSAP address prefix forces the prefixes to be added to the BGP routing table. To configure advertisement of networking prefixes, perform the steps in this procedure.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router bgp as-number`
4. `no bgp default ipv4-unicast`
5. `neighbor {ip-address | peer-group-name} remote-as as-number`
6. `address-family nsap [unicast]`
7. `network nsap-prefix [route-map map-tag]`
8. `neighbor ip-address activate`
9. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode.
	Example: Router> enable	• Enter your password if prompted.
Step 2	<code>configure terminal</code>	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	<code>router bgp as-number</code> Example: Router(config)# router bgp 65101	Configures a BGP routing process and enters router configuration mode for the specified routing process.
Step 4	<code>no bgp default ipv4-unicast</code> Example: Router(config-router)# no bgp default ipv4-unicast	Disables the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers.
Step 5	<code>neighbor {ip-address peer-group-name} remote-as as-number</code> Example: Router(config-router)# neighbor 10.1.2.2 remote-as 64202	Adds an IP address or peer group name of the BGP neighbor in the specified autonomous system to the BGP neighbor table of the local router.
Step 6	<code>address-family nsap [unicast]</code> Example: Router(config-router)# address-family nsap	Specifies the NSAP address family and enters address family configuration mode. The optional unicast keyword specifies the NSAP unicast address prefixes. By default, the router is placed in unicast NSAP address family configuration mode if the unicast keyword is not specified with the address-family nsap command.
Step 7	<code>network nsap-prefix [route-map map-tag]</code> Example: Router(config-router-af)# network 49.0101.1111.1111.1111.1111.00	Advertises a single prefix of the local OSI routing domain and enters it in the BGP routing table. Note It is possible to advertise a single prefix, in which case this prefix could be the unique NSAP address prefix of the local OSI routing domain. Alternatively, multiple longer prefixes, each covering a small portion of the OSI routing domain, can be used to selectively advertise different areas. The advertising of NSAP address prefixes can be controlled by using the optional route-map keyword. If no route map is specified, all NSAP address prefixes are redistributed.
Step 8	<code>neighbor ip-address activate</code> Example: Router(config-router-af) neighbor 10.1.2.2 activate	Specifies that NSAP routing information will be sent to the specified BGP neighbor. Note See the description of the neighbor command in the documents listed in the “Additional References” section on page 35 for more details on the use of this command.
Step 9	<code>end</code> Example: Router(config-router-af)# end	Exits address family configuration mode and returns to privileged EXEC mode.

Redistributing Routes from BGP into IS-IS

Route redistribution must be approached with caution. We do not recommend injecting the full set of BGP routes into IS-IS because excessive routing traffic will be added to IS-IS. Route maps can be used to control which dynamic routes are redistributed.

To configure route redistribution from BGP into IS-IS, perform the steps in this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis area-tag**
4. **net network-entity-title**
5. **redistribute protocol as-number [route-type] [route-map map-tag]**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router isis area-tag Example: Router(config)# router isis osi-as-404	Configures an IS-IS routing process and enters router configuration mode for the specified routing process. Note You cannot redistribute BGP routes into a Level 1-only IS-IS routing process.
Step 4	net network-entity-title Example: Router(config-router)# net 49.0404.7777.7777.7777.00	Configures a network entity title (NET) for the routing process. If you are configuring multiarea IS-IS, you must specify a NET for each routing process.

	Command or Action	Purpose
Step 5	<code>redistribute protocol as-number [route-type] [route-map map-tag]</code> Example: <code>Router(config-router)# redistribute bgp 65404 clns</code>	Redistributes NSAP prefix routes from BGP into the CLNS Level 2 routing table associated with the IS-IS routing process when the <i>protocol</i> argument is set to bgp and the <i>route-type</i> argument is set to clns . - The <i>as-number</i> argument is defined as the autonomous system number of the BGP routing process to be redistributed into CLNS. - The redistribution of routes can be controlled by using the optional route-map keyword. If no route map is specified, all BGP routes are redistributed.
Step 6	<code>end</code> Example: <code>Router(config-router)# end</code>	Exits router configuration mode and returns to privileged EXEC mode.

Redistributing Routes from IS-IS into BGP

Route redistribution must be approached with caution because redistributed route information is stored in the routing tables. Large routing tables may make the routing process slower. Route maps can be used to control which dynamic routes are redistributed.

To configure route redistribution from IS-IS into BGP, perform the steps in this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **address-family nsap** [**unicast**]
6. **redistribute protocol** [*process-id*] [*route-type*] [**route-map** *map-tag*]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: <code>Router# configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>router bgp as-number</code> Example: Router(config)# router bgp 65202	Configures a BGP routing process and enters router configuration mode for the specified routing process.
Step 4	<code>no bgp default ipv4-unicast</code> Example: Router(config-router)# no bgp default ipv4-unicast	Disables the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers.
Step 5	<code>address-family nsap [unicast]</code> Example: Router(config-router)# address-family nsap	Specifies the NSAP address family and enters address family configuration mode.
Step 6	<code>redistribute protocol [process-id] [route-type] [route-map map-tag]</code> Example: Router(config-router-af)# redistribute isis osi-as-202 clns route-map internal-routes-only	Redistributes routes from the CLNS Level 2 routing table associated with the IS-IS routing process into BGP as NSAP prefixes when the <i>protocol</i> argument is set to isis and the <i>route-type</i> argument is set to clns . - The <i>process-id</i> argument is defined as the area name for the relevant IS-IS routing process to be redistributed. - The redistribution of routes can be controlled by using the optional route-map keyword. If no route map is specified, all Level 2 routes are redistributed.
Step 7	<code>end</code> Example: Router(config-router-af)# end	Exits address family configuration mode and returns to privileged EXEC mode.

Configuring BGP Peer Groups and Route Reflectors

BGP peer groups reduce the number of configuration commands by applying a BGP **neighbor** command to multiple neighbors. Using a BGP peer group with a local router configured as a BGP route reflector allows BGP routing information received from one member of the group to be replicated to all other group members. Without a peer group, each route reflector client must be specified by IP address.

To create a BGP peer group and use the group as a BGP route reflector client, perform the steps in this procedure. This is an optional task and is used with internal BGP neighbors. In this task, some of the BGP syntax is shown with the *peer-group-name* argument only and only one neighbor is configured as a member of the peer group. Repeat Step 9 to configure other BGP neighbors as members of the peer group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp as-number**
4. **no bgp default ipv4-unicast**

5. **neighbor** *peer-group-name* **peer-group**
6. **neighbor** *peer-group-name* **remote-as** *as-number*
7. **address-family** *nsap* [*unicast*]
8. **neighbor** *peer-group-name* **route-reflector-client**
9. **neighbor** *ip-address* **peer-group** *peer-group-name*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router bgp <i>as-number</i> Example: Router(config)# router bgp 65303	Configures a BGP routing process and enters router configuration mode for the specified routing process.
Step 4	no bgp default ipv4-unicast Example: Router(config-router)# no bgp default ipv4-unicast	Disables the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers.
Step 5	neighbor <i>peer-group-name</i> peer-group Example: Router(config-router)# neighbor ibgp-peers peer-group	Creates a BGP peer group.
Step 6	neighbor <i>peer-group-name</i> remote-as <i>as-number</i> Example: Router(config-router)# neighbor ibgp-peers remote-as 65303	Adds the peer group name of the BGP neighbor in the specified autonomous system to the BGP neighbor table of the local router.
Step 7	address-family <i>nsap</i> [<i>unicast</i>] Example: Router(config-router)# address-family nsap	Specifies the NSAP address family and enters address family configuration mode.
Step 8	neighbor <i>peer-group-name</i> route-reflector-client Example: Router(config-router-af)# neighbor ibgp-peers route-reflector-client	Configures the router as a BGP route reflector and configures the specified peer group as its client.

	Command or Action	Purpose
Step 9	<code>neighbor ip-address peer-group peer-group</code> Example: Router(config-router-af)# neighbor 10.4.5.4 peer-group ibgp-peers	Assigns a BGP neighbor to a BGP peer group.
Step 10	<code>end</code> Example: Router(config-router-af)# end	Exits address family configuration mode and returns to privileged EXEC mode.

Filtering Inbound Routes Based on NSAP Prefixes

Perform this task to filter inbound BGP routes based on NSAP prefixes. The **neighbor prefix-list in** command is configured in address family configuration mode to filter inbound routes.

Prerequisites

You must specify either a CLNS filter set or a CLNS filter expression before configuring the **neighbor** command. See descriptions for the **clns filter-expr** and **clns filter-set** commands for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp as-number**
4. **no bgp default ipv4-unicast**
5. **address-family nsap [unicast]**
6. **neighbor {ip-address | peer-group-name} prefix-list {clns-filter-expr-name | clns-filter-set-name} in**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>router bgp as-number</code> Example: Router(config)# router bgp 65200	Configures a BGP routing process and enters router configuration mode for the specified routing process.
Step 4	<code>no bgp default ipv4-unicast</code> Example: Router(config-router)# no bgp default ipv4-unicast	Disables the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers.
Step 5	<code>address-family nsap [unicast]</code> Example: Router(config-router)# address-family nsap	Specifies the address family and enters address family configuration mode.
Step 6	<code>neighbor {ip-address peer-group-name} prefix-list {clns-filter-expr-name clns-filter-set-name} in</code> Example: Router(config-router-af)# neighbor 10.23.4.1 prefix-list abc in	Specifies a CLNS filter set or CLNS filter expression to be used to filter inbound BGP routes. - The <i>clns-filter-expr-name</i> argument is defined with the clns filter-expr configuration command. - The <i>clns-filter-set-name</i> argument is defined with the clns filter-set configuration command.
Step 7	<code>end</code> Example: Router(config-router-af)# end	Exits address family configuration mode and returns to privileged EXEC mode.

Filtering Outbound BGP Updates Based on NSAP Prefixes

Perform this task to filter outbound BGP updates based on NSAP prefixes, use the **neighbor prefix-list out** command in address family configuration mode. This task is configured at Router 7 in [Figure 1](#). In this task, a CLNS filter is created with two entries to deny NSAP prefixes starting with 49.0404 and to permit all other NSAP prefixes starting with 49. A BGP peer group is created and the filter is applied to outbound BGP updates for the neighbor that is a member of the peer group.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `clns filter-set name [deny] template`
4. `clns filter-set name [permit] template`
5. `router bgp as-number`
6. `no bgp default ipv4-unicast`
7. `neighbor peer-group-name peer-group`
8. `neighbor {ip-address | peer-group-name} remote-as as-number`
9. `address-family nsap [unicast]`

10. **neighbor** {*ip-address* | *peer-group-name*} **prefix-list** {*clns-filter-expr-name* | *clns-filter-set-name*} **out**
11. **neighbor** *ip-address* **peer-group** *peer-group-name*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	clns filter-set name [deny] template Example: Router(config)# clns filter-set routes0404 deny 49.0404...	Defines a NSAP prefix match for a deny condition for use in CLNS filter expressions. In this example, a deny action is returned if an address starts with 49.0404.
Step 4	clns filter-set name [permit] template Example: Router(config)# clns filter-set routes0404 permit 49...	Defines a NSAP prefix match for a permit condition for use in CLNS filter expressions. In this example, a permit action is returned if an address starts with 49. Note Although the permit example in this step allows all NSAP addresses starting with 49, the match condition in Step 3 is processed first so the NSAP addresses starting with 49.0404 are still denied.
Step 5	router bgp as-number Example: Router(config)# router bgp 65404	Configures a BGP routing process and enters router configuration mode for the specified routing process.
Step 6	no bgp default ipv4-unicast Example: Router(config-router)# no bgp default ipv4-unicast	Disables the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers.
Step 7	neighbor peer-group-name peer-group Example: Router(config-router)# neighbor ebgp-peers peer-group	Creates a BGP peer group. In this example, the BGP peer group named ebgp-peers is created.

	Command or Action	Purpose
Step 8	<pre>neighbor {ip-address peer-group-name} remote-as as-number</pre> Example: <pre>Router(config-router)# neighbor ebgp-peers remote-as 65303</pre>	Adds an IP address or peer group name of the BGP neighbor in the specified autonomous system to the BGP neighbor table of the local router. In this example, the peer group named ebgp-peers is added to the BGP neighbor table.
Step 9	<pre>address-family nsap [unicast]</pre> Example: <pre>Router(config-router)# address-family nsap</pre>	Specifies the NSAP address family and enters address family configuration mode.
Step 10	<pre>neighbor {ip-address peer-group-name} prefix-list {clns-filter-expr-name clns-filter-set-name} out</pre> Example: <pre>Router(config-router-af)# neighbor ebgp-peers prefix-list routes0404 out</pre>	Specifies a CLNS filter set or CLNS filter expression to be used to filter outbound BGP updates. - The <i>clns-filter-expr-name</i> argument is defined with the clns filter-expr configuration command. - The <i>clns-filter-set-name</i> argument is defined with the clns filter-set configuration command. - In this example, the filter set named routes0404 was created in Step 3 and Step 4.
Step 11	<pre>neighbor ip-address peer-group peer-group</pre> Example: <pre>Router(config-router-af)# neighbor 10.6.7.8 peer-group ebgp-peers</pre>	Assigns a BGP neighbor to a BGP peer group.
Step 12	<pre>end</pre> Example: <pre>Router(config-router-af)# end</pre>	Exits address family configuration mode and returns to privileged EXEC mode.

Originating Default Routes for a Neighboring Routing Domain

To create a default CLNS route that points to the local router on behalf of a neighboring OSI routing domain, perform the steps in this procedure. This is an optional task and is normally used only with external BGP neighbors.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp as-number**
4. **no bgp default ipv4-unicast**
5. **address-family nsap [unicast]**
6. **neighbor {ip-address | peer-group-name} default-originate [route-map map-tag]**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router bgp <i>as-number</i> Example: Router(config)# router bgp 64803	Configures a BGP routing process and enters router configuration mode for the specified routing process.
Step 4	no bgp default ipv4-unicast Example: Router(config-router)# no bgp default ipv4-unicast	Disables the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers.
Step 5	address-family nsap [<i>unicast</i>] Example: Router(config-router)# address-family nsap	Specifies the NSAP address family and enters address family configuration mode.
Step 6	neighbor { <i>ip-address</i> <i>peer-group-name</i> } default-originate [<i>route-map</i> <i>map-tag</i>] Example: Router(config-router-af)# neighbor 172.16.2.3 default-originate	Generates a default CLNS route that points to the local router and that will be advertised to the neighboring OSI routing domain.
Step 7	end Example: Router(config-router-af)# end	Exits address family configuration mode and returns to privileged EXEC mode.

Verifying MP-BGP Support for CLNS

To verify the configuration, use the **show running-config** EXEC command. Sample output is located in the [“Implementing MP-BGP Support for CLNS: Example”](#) section on page 30. To verify that the Multiprotocol BGP (MP-BGP) Support for CLNS feature is working, perform the following steps.

SUMMARY STEPS

1. **show clns neighbors**
2. **show clns route**

3. **show bgp nsap unicast summary**
4. **show bgp nsap unicast**

DETAILED STEPS

Step 1 **show clns neighbors**

Use this command to confirm that the local router has formed all the necessary IS-IS adjacencies with other Level 2 IS-IS routers in the local OSI routing domain. If the local router has any directly connected external BGP peers, the output from this command will show that the external neighbors have been discovered, in the form of ES-IS adjacencies.

In the following example, the output is displayed for router R2, shown in [Figure 1 on page 3](#). R2 has three CLNS neighbors. R1 and R4 are ES-IS neighbors because these nodes are in different autonomous systems from R2. R3 is an IS-IS neighbor because it is in the same autonomous system as R2. Note that the system ID is replaced by CLNS hostnames (r1, r3, and r4) that are defined at the start of each configuration file. Specifying the CLNS hostname means that you need not remember which system ID corresponds to which hostname.

```
Router# show clns neighbors
```

```
Tag osi-as-202:
System Id      Interface  SNPA                State  Holdtime  Type Protocol
r1             Se2/0     *HDLC*              Up     274       IS   ES-IS
r3             Et0/1     0002.16de.8481      Up     9         L2   IS-IS
r4             Se2/2     *HDLC*              Up     275       IS   ES-IS
```

Step 2 **show clns route**

Use this command to confirm that the local router has calculated routes to other areas in the local OSI routing domain. In the following example of output from router R2, shown in [Figure 1 on page 3](#), the routing table entry—i 49.0202.3333 [110/10] via R3—shows that router R2 knows about other local IS-IS areas within the local OSI routing domain.

```
Router# show clns route
```

```
Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP, i - IS-IS, e - ES-IS
       B - BGP,      b - eBGP-neighbor

C 49.0202.2222 [2/0], Local IS-IS Area
C 49.0202.2222.2222.2222.2222.00 [1/0], Local IS-IS NET

b 49.0101.1111.1111.1111.1111.00 [15/10]
   via r1, Serial2/0
i 49.0202.3333 [110/10]
   via r3, Ethernet0/1
b 49.0303.4444.4444.4444.4444.00 [15/10]
   via r4, Serial2/2
B 49.0101 [20/1]
   via r1, Serial2/0
B 49.0303 [20/1]
   via r4, Serial2/2
B 49.0404 [200/1]
   via r9
i 49.0404.9999.9999.9999.9999.00 [110/10]
   via r3, Ethernet0/1
```

Step 3 **show bgp nsap unicast summary**

Use this command to verify that the TCP connection to a particular neighbor is active. In the following example output, search the appropriate row based on the IP address of the neighbor. If the State/PfxRcd column entry is a number, including zero, the TCP connection for that neighbor is active.

```
Router# show bgp nsap unicast summary
```

```
BGP router identifier 10.1.57.11, local AS number 65202
BGP table version is 6, main routing table version 6
5 network entries and 8 paths using 1141 bytes of memory
6 BGP path attribute entries using 360 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 5/0 prefixes, 8/0 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.2.1	4	65101	34	34	6	0	0	00:29:11	1
10.2.3.3	4	65202	35	36	6	0	0	00:29:16	3

- Step 4** Enter the **show bgp nsap unicast** command to display all the NSAP prefix routes that the local router has discovered. In the following example of output from router R2, shown in [Figure 1 on page 3](#), a single valid route to prefix 49.0101 is shown. Two valid routes—marked by a *—are shown for the prefix 49.0404. The second route is marked with a *>i sequence, representing the best route to this prefix.

```
Router# show bgp nsap unicast
```

```
BGP table version is 3, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 49.0101	49.0101.1111.1111.1111.1111.00			0	65101 i
* i49.0202.2222	49.0202.3333.3333.3333.3333.00		100	0	?
*>	49.0202.2222.2222.2222.2222.00			32768	?
* i49.0202.3333	49.0202.3333.3333.3333.3333.00		100	0	?
*>	49.0202.2222.2222.2222.2222.00			32768	?
*> 49.0303	49.0303.4444.4444.4444.4444.00			0	65303 i
* 49.0404	49.0303.4444.4444.4444.4444.00			0	65303 65404 i
*>i	49.0404.9999.9999.9999.9999.00		100	0	65404 i

Troubleshooting MP-BGP Support for CLNS

The **debug bgp nsap unicast** commands enable diagnostic output concerning various events relating to the operation of the CLNS packets in the BGP routing protocol to be displayed on a console. These commands are intended only for troubleshooting purposes because the volume of output generated by the software when they are used can result in severe performance degradation on the router. See the *Cisco IOS Debug Command Reference* for more information about using these **debug** commands.

To troubleshoot problems with the configuration of MP-BGP support for CLNS and to minimize the impact of the **debug** commands used in this procedure, perform the following steps.

SUMMARY STEPS

1. Attach a console.
2. **no logging console**
3. Use Telnet to access a router port.
4. **enable**
5. **terminal monitor**
6. **debug bgp nsap unicast** [*neighbor-address* | **dampening** | **keepalives** | **updates**]
7. **no terminal monitor**
8. **no debug bgp nsap unicast** [*neighbor-address* | **dampening** | **keepalives** | **updates**]
9. **logging console**

DETAILED STEPS

- Step 1** Attach a console directly to a router running the Cisco IOS software release that includes the Multiprotocol BGP (MP-BGP) Support for CLNS feature.



Note This procedure will minimize the load on the router created by the **debug bgp nsap unicast** commands because the console port will no longer be generating character-by-character processor interrupts. If you cannot connect to a console directly, you can run this procedure via a terminal server. If you must break the Telnet connection, however, you may not be able to reconnect because the router may be unable to respond due to the processor load of generating the **debug bgp nsap unicast** output.

- Step 2** **no logging console**
This command disables all logging to the console terminal.
- Step 3** Use Telnet to access a router port.
- Step 4** **enable**
Enter this command to access privileged EXEC mode.
- Step 5** **terminal monitor**
This command enables logging on the virtual terminal.
- Step 6** **debug bgp nsap unicast** [*neighbor-address* | **dampening** | **keepalives** | **updates**]
Enter only specific **debug bgp nsap unicast** commands to isolate the output to a certain subcomponent and minimize the load on the processor. Use appropriate arguments and keywords to generate more detailed debug information on specified subcomponents.
- Step 7** **no terminal monitor**
This command disables logging on the virtual terminal.
- Step 8** **no debug bgp nsap unicast** [*neighbor-address* | **dampening** | **keepalives** | **updates**]
Enter the specific **no debug bgp nsap unicast** command when you are finished.

Step 9 logging console

This command reenables logging to the console.

Configuration Examples for MP-BGP Support for CLNS

This section provides configuration examples to match the identified configuration tasks in the previous section. To provide an overview of all the router configurations in [Figure 1 on page 3](#), more detailed configurations for each router are added at the end of this section.

- [Configuring and Activating a BGP Neighbor to Support CLNS: Example, page 26](#)
- [Configuring an IS-IS Routing Process: Example, page 27](#)
- [Configuring Interfaces: Example, page 27](#)
- [Advertising Networking Prefixes: Example, page 27](#)
- [Redistributing Routes from BGP into IS-IS: Example, page 27](#)
- [Redistributing Routes from IS-IS into BGP: Example, page 28](#)
- [Configuring BGP Peer Groups and Route Reflectors: Example, page 28](#)
- [Filtering Inbound Routes Based on NSAP Prefixes: Example, page 28](#)
- [Filtering Outbound BGP Updates Based on NSAP Prefixes: Example, page 29](#)
- [Originating a Default Route and Outbound Route Filtering: Example, page 29](#)
- [Implementing MP-BGP Support for CLNS: Example, page 30](#)

Configuring and Activating a BGP Neighbor to Support CLNS: Example

In the following example, the router R1, shown in [Figure 3 on page 30](#), in the autonomous system AS65101 is configured to run BGP and activated to support CLNS. Router R1 is the only Level 2 IS-IS router in autonomous system AS65101, and it has only one connection to another autonomous system via router R2 in AS65202. The **no bgp default ipv4-unicast** command is configured on the router to disable the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers. After the NSAP address family configuration mode is enabled with the **address-family nsap** command, the router is configured to advertise the NSAP prefix of 49.0101 to its BGP neighbors and to send NSAP routing information to the BGP neighbor at 10.1.2.2.

```
router bgp 65101
no bgp default ipv4-unicast
address-family nsap
network 49.0101...
neighbor 10.1.2.2 activate
exit-address-family
```

Configuring an IS-IS Routing Process: Example

In the following example, the router R1, shown in [Figure 3 on page 30](#), is configured to run an IS-IS process:

```
router isis osi-as-101
 net 49.0101.1111.1111.1111.00
```

The default IS-IS routing process level is used.

Configuring Interfaces: Example

In the following example, two of the interfaces of the router R2, shown in [Figure 3 on page 30](#), in the autonomous system AS65202 are configured to run CLNS. Ethernet interface 0/1 is connected to the local OSI routing domain and is configured to run IS-IS when the network protocol is CLNS using the **clns router isis** command. The serial interface 2/0 with the local IP address of 10.1.2.2 is connected with an eBGP neighbor and is configured to run CLNS through the **clns enable** command:

```
interface serial 2/0
 ip address 10.1.2.2 255.255.255.0
 clns enable
 no shutdown
!
interface ethernet 0/1
 ip address 10.2.3.1 255.255.255.0
 clns router isis osi-as-202
 no shutdown
```

Advertising Networking Prefixes: Example

In the following example, the router R1, shown in [Figure 3 on page 30](#), is configured to advertise the NSAP prefix of 49.0101 to other routers. The NSAP prefix unique to autonomous system AS65101 is advertised to allow the other autonomous systems to discover the existence of autonomous system AS65101 in the network:

```
router bgp 65101
 no bgp default ipv4-unicast
 neighbor 10.1.2.2 remote-as 64202
 address-family nsap
  network 49.0101...
 neighbor 10.1.2.2 activate
```

Redistributing Routes from BGP into IS-IS: Example

In the following example, the routers R7 and R9, shown in [Figure 3 on page 30](#), in the autonomous system AS65404 are configured to redistribute BGP routes into the IS-IS routing process called osi-as-404. Redistributing the BGP routes allows the Level 2 IS-IS router, R8, to advertise routes to destinations outside the autonomous system AS65404. Without a route map being specified, all BGP routes are redistributed.

Router R7

```
router isis osi-as-404
 net 49.0404.7777.7777.7777.00
 redistribute bgp 65404 clns
```

Router R9

```
router isis osi-as-404
 net 49.0404.9999.9999.9999.00
 redistribute bgp 65404 clns
```

Redistributing Routes from IS-IS into BGP: Example

In the following example, the router R2, shown in [Figure 3 on page 30](#), in the autonomous system AS65202 is configured to redistribute Level 2 CLNS NSAP routes into BGP. A route map is used to permit only routes from within the local autonomous system to be redistributed into BGP. Without a route map being specified, every NSAP route from the CLNS level 2 prefix table is redistributed. The **no bgp default ipv4-unicast** command is configured on the router to disable the default behavior of the BGP routing process exchanging IPv4 addressing information with BGP neighbor routers.

```
clns filter-set internal-routes permit 49.0202...
!
route-map internal-routes-only permit 10
 match clns address internal-routes
!
router isis osi-as-202
 net 49.0202.2222.2222.2222.00
!
router bgp 65202
 no bgp default ipv4-unicast
 address-family nsap
 redistribute isis osi-as-202 clns route-map internal-routes-only
```

Configuring BGP Peer Groups and Route Reflectors: Example

Router R5, shown in [Figure 1 on page 3](#), has only iBGP neighbors and runs IS-IS on both interfaces. To reduce the number of configuration commands, configure R5 as a member of a BGP peer group called **ibgp-peers**. The peer group is automatically activated under the **address-family nsap** command by configuring the peer group as a route reflector client allowing it to exchange NSAP routing information between group members. The BGP peer group is also configured as a BGP route reflector client to reduce the need for every iBGP router to be linked to each other.

In the following example, the router R5 in the autonomous system AS65303 is configured as a member of a BGP peer group and a BGP route reflector client.

```
router bgp 65303
 no bgp default ipv4-unicast
 neighbor ibgp-peers peer-group
 neighbor ibgp-peers remote-as 65303
 address-family nsap
  neighbor ibgp-peers route-reflector-client
 neighbor 10.4.5.4 peer-group ibgp-peers
 neighbor 10.5.6.6 peer-group ibgp-peers
 exit-address-family
```

Filtering Inbound Routes Based on NSAP Prefixes: Example

In the following example, the router R1, shown in [Figure 3 on page 30](#), in the autonomous system AS65101 is configured to filter inbound routes specified by the default-prefix-only prefix list.

```
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
```

```

!
router isis osi-as-101
 net 49.0101.1111.1111.1111.1111.00
!
router bgp 65101
 no bgp default ipv4-unicast
 neighbor 10.1.2.2 remote-as 64202
 address-family nsap
  network 49.0101.1111.1111.1111.1111.00
  neighbor 10.1.2.2 activate
  neighbor 10.1.2.2 prefix-list default-prefix-only in

```

Filtering Outbound BGP Updates Based on NSAP Prefixes: Example

In the following example, outbound BGP updates are filtered based on NSAP prefixes. This example is configured at Router 7 in [Figure 3 on page 30](#). In this task, a CLNS filter is created with two entries to deny NSAP prefixes starting with 49.0404 and to permit all other NSAP prefixes starting with 49. A BGP peer group is created and the filter is applied to outbound BGP updates for the neighbor that is a member of the peer group.

```

clns filter-set routes0404 deny 49.0404...
clns filter-set routes0404 permit 49...
!
router bgp 65404
 no bgp default ipv4-unicast
 neighbor ebgp-peers remote-as 65303
 address-family nsap
  neighbor ebgp-peers prefix-list routes0404 out
  neighbor 10.6.7.8 peer-group ebgp-peers

```

Originating a Default Route and Outbound Route Filtering: Example

In [Figure 3 on page 30](#), autonomous system AS65101 is connected to only one other autonomous system, AS65202. Router R2 in AS65202 provides the connectivity to the rest of the network for autonomous system AS65101 by sending a default route to R1. Any packets from Level 1 routers within autonomous system AS65101 with destination NSAP addresses outside the local Level 1 network are sent to R1, the nearest Level 2 router. Router R1 forwards the packets to router R2 using the default route.

In the following example, the router R2, shown in [Figure 3 on page 30](#), in the autonomous system AS65202 is configured to generate a default route for router R1 in the autonomous system AS65101, and an outbound filter is created to send only the default route NSAP addressing information in the BGP update messages to router R1.

```

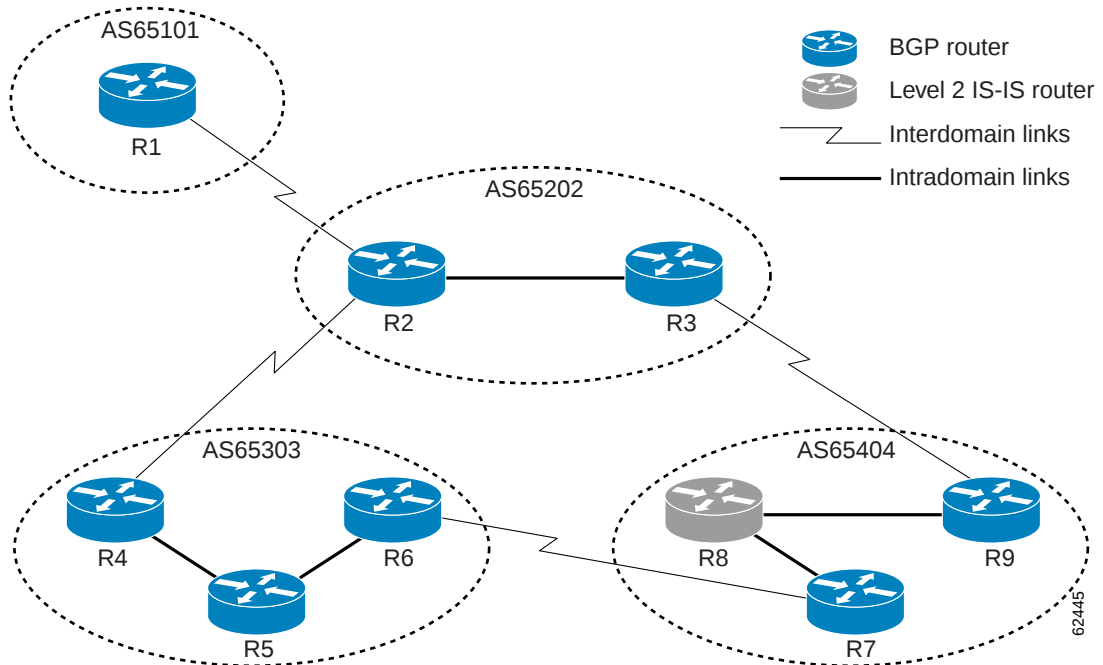
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
router bgp 65202
 no bgp default ipv4-unicast
 neighbor 10.1.2.1 remote-as 64101
 address-family nsap
  network 49.0202...
  neighbor 10.1.2.1 activate
  neighbor 10.1.2.1 default-originate
  neighbor 10.1.2.1 prefix-list default-prefix-only out

```

Implementing MP-BGP Support for CLNS: Example

Figure 3 shows a generic BGP CLNS network containing nine routers that are grouped into four different autonomous systems (in BGP terminology) or routing domains (in OSI terminology). This section contains complete configurations for all routers shown in Figure 3.

Figure 3 Components in a Generic BGP CLNS Network



If you need more details about commands used in the following examples, see the configuration tasks earlier in this document and the documents listed in the [“Additional References”](#) section on page 35.

Autonomous System AS65101

Router 1

```

clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
router isis osi-as-101
 net 49.0101.1111.1111.1111.1111.00
!
router bgp 65101
 no bgp default ipv4-unicast
 neighbor 10.1.2.2 remote-as 65202
 address-family nsap
  neighbor 10.1.2.2 activate
  neighbor 10.1.2.2 prefix-list default-prefix-only in
 network 49.0101...
 exit-address-family
!
interface serial 2/0
 ip address 10.1.2.1 255.255.255.0
 clns enable
 no shutdown

```

Autonomous System AS65202

Router 2

```

clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
clns filter-set internal-routes permit 49.0202...
!
route-map internal-routes-only permit 10
    match clns address internal-routes
!
router isis osi-as-202
    net 49.0202.2222.2222.2222.00
!
router bgp 65202
    no bgp default ipv4-unicast
    neighbor 10.1.2.1 remote-as 65101
    neighbor 10.2.3.3 remote-as 65202
    neighbor 10.2.4.4 remote-as 65303
    address-family nsap
        neighbor 10.1.2.1 activate
        neighbor 10.2.3.3 activate
        neighbor 10.2.4.4 activate
        redistribute isis osi-as-202 clns route-map internal-routes-only
        neighbor 10.1.2.1 default-originate
        neighbor 10.1.2.1 prefix-list default-prefix-only out
    exit-address-family

!
interface ethernet 0/1
    ip address 10.2.3.2 255.255.255.0
    clns router isis osi-as-202
    no shutdown
!
interface serial 2/0
    ip address 10.1.2.2 255.255.255.0
    clns enable
    no shutdown
!
interface serial 2/2
    ip address 10.2.4.2 255.255.255.0
    clns enable
    no shutdown
    
```

Router 3

```

clns filter-set internal-routes permit 49.0202...
!
route-map internal-routes-only permit 10
    match clns address internal-routes
!
router isis osi-as-202
    net 49.0202.3333.3333.3333.00
!
router bgp 65202
    no bgp default ipv4-unicast
    neighbor 10.2.3.2 remote-as 65202
    neighbor 10.3.9.9 remote-as 65404
    address-family nsap
        neighbor 10.2.3.2 activate
        neighbor 10.3.9.9 activate
        redistribute isis osi-as-202 clns route-map internal-routes-only
    exit-address-family
    
```

```

!
interface ethernet 0/1
 ip address 10.2.3.3 255.255.255.0
 clns router isis osi-as-202
 no shutdown
!
interface serial 2/2
 ip address 10.3.9.3 255.255.255.0
 clns enable
 no shutdown

```

Autonomous System AS65303

Router 4

```

router isis osi-as-303
 net 49.0303.4444.4444.4444.4444.00
!
router bgp 65303
 no bgp default ipv4-unicast
 neighbor 10.2.4.2 remote-as 65202
 neighbor 10.4.5.5 remote-as 65303
 address-family nsap
  no synchronization
  neighbor 10.2.4.2 activate
  neighbor 10.4.5.5 activate
 network 49.0303...
 exit-address-family
!
interface ethernet 0/2
 ip address 10.4.5.4 255.255.255.0
 clns router isis osi-as-303
 no shutdown
!
interface serial 2/3
 ip address 10.2.4.4 255.255.255.0
 clns enable
 no shutdown

```

Router 5

```

router isis osi-as-303
 net 49.0303.5555.5555.5555.5555.00
!
router bgp 65303
 no bgp default ipv4-unicast
 neighbor ibgp-peers peer-group
 neighbor ibgp-peers remote-as 65303
 address-family nsap
  no synchronization
  neighbor ibgp-peers route-reflector-client
  neighbor 10.4.5.4 peer-group ibgp-peers
  neighbor 10.5.6.6 peer-group ibgp-peers
 exit-address-family
!
interface ethernet 0/2
 ip address 10.4.5.5 255.255.255.0
 clns router isis osi-as-303
 no shutdown
!

```

```
interface ethernet 0/3
 ip address 10.5.6.5 255.255.255.0
 clns router isis osi-as-303
 no shutdown
```

Router 6

```
router isis osi-as-303
 net 49.0303.6666.6666.6666.6666.00
!
router bgp 65303
 no bgp default ipv4-unicast
 neighbor 10.5.6.5 remote-as 65303
 neighbor 10.6.7.7 remote-as 65404
 address-family nsap
  no synchronization
  neighbor 10.5.6.5 activate
  neighbor 10.6.7.7 activate
  network 49.0303...
!
interface ethernet 0/3
 ip address 10.5.6.6 255.255.255.0
 clns router isis osi-as-303
 no shutdown
!
interface serial 2/2
 ip address 10.6.7.6 255.255.255.0
 clns enable
 no shutdown
```

Autonomous System AS65404

Router 7

```
clns filter-set external-routes deny 49.0404...
clns filter-set external-routes permit 49...
!
route-map noexport permit 10
 match clns address external-routes
 set community noexport
!
router isis osi-as-404
 net 49.0404.7777.7777.7777.7777.00
 redistribute bgp 404 clns
!
router bgp 65404
 no bgp default ipv4-unicast
 neighbor 10.6.7.6 remote-as 65303
 neighbor 10.8.9.9 remote-as 65404
 address-family nsap
  neighbor 10.6.7.6 activate
  neighbor 10.8.9.9 activate
  neighbor 10.8.9.9 send-community
  neighbor 10.8.9.9 route-map noexport out
  network 49.0404...
!
interface ethernet 1/0
 ip address 10.7.8.7 255.255.255.0
 clns router isis osi-as-404
 ip router isis osi-as-404
 no shutdown
!
interface serial 2/3
```

```

ip address 10.6.7.7 255.255.255.0
clns enable
no shutdown

```

Router 8

```

router isis osi-as-404
 net 49.0404.8888.8888.8888.8888.00
!
interface ethernet 1/0
 ip address 10.7.8.8 255.255.255.0
 clns router isis osi-as-404
 ip router isis osi-as-404
 no shutdown
!
interface ethernet 1/1
 ip address 10.8.9.8 255.255.255.0
 clns router isis osi-as-404
 ip router isis osi-as-404
 no shutdown

```

Router 9

```

clns filter-set external-routes deny 49.0404...
clns filter-set external-routes permit 49...
!
route-map noexport permit 10
 match clns address external-routes
 set community noexport
!
router isis osi-as-404
 net 49.0404.9999.9999.9999.9999.00
 redistribute bgp 404 clns
!
router bgp 65404
 no bgp default ipv4-unicast
 neighbor 10.3.9.3 remote-as 65202
 neighbor 10.7.8.7 remote-as 65404
 address-family nsap
  network 49.0404...
  neighbor 10.3.9.3 activate
  neighbor 10.7.8.7 activate
  neighbor 10.7.8.7 send-community
  neighbor 10.7.8.7 route-map noexport out
!
interface serial 2/3
 ip address 10.3.9.9 255.255.255.0
 clns enable
 no shutdown
!
interface ethernet 1/1
 ip address 10.8.9.9 255.255.255.0
 clns router isis osi-as-404
 ip router isis osi-as-404
 no shutdown

```

Additional References

The following sections provide references related to the Multiprotocol BGP (MP-BGP) Support for CLNS feature.

Related Documents

Related Topic	Document Title
BGP commands	• Cisco IOS IP Routing Protocols Command Reference, Release 12.2 SR • Cisco IOS IP Routing Protocols Command Reference, Release 12.4T
CLNS commands	• Cisco IOS ISO CLNS Command Reference, Release 12.2 SR • Cisco IOS ISO CLNS Command Reference, Release 12.4T

Standards

Standard	Title
ISO/IEC 8473	<i>ISO CLNP: Connectionless Network Protocol (ISO-IP)</i> . Protocol for providing the connectionless-mode network service.
ISO/IEC 9542	<i>End System to Intermediate System Protocol (ESIS)</i> . End system to Intermediate system routing exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473).
ISO/IEC 10589	<i>IS-IS, Intermediate System-to-Intermediate System</i> . Intermediate system to Intermediate system intradomain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473).

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1700	<i>Assigned Numbers</i>
RFC 1771	<i>A Border Gateway Protocol 4 (BGP-4)</i>

RFC	Title
RFC 1997	<i>BGP Communities Attribute</i>
RFC 2042	<i>Registering New BGP Attribute Types</i>
RFC 2439	<i>BGP Route Flap Dampening</i>
RFC 2842	<i>Capabilities Advertisement with BGP-4</i>
RFC 2858	<i>Multiprotocol Extensions for BGP-4</i>
RFC 2918	<i>Route Refresh Capability for BGP-4</i>

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Configuring MP-BGP Support for CLNS

[Table 1](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 **Feature Information for MP-BGP Support for CLNS**

Feature Name	Releases	Feature Information
Multiprotocol BGP (MP-BGP) Support for CLNS	12.2(8)T 12.2(33)SRB	The Multiprotocol BGP (MP-BGP) Support for CLNS feature provides the ability to scale Connectionless Network Service (CLNS) networks. The multiprotocol extensions of Border Gateway Protocol (BGP) add the ability to interconnect separate Open System Interconnection (OSI) routing domains without merging the routing domains, thus providing the capability to build very large OSI networks. In Release 12.2(8)T, this feature was introduced on the following platforms: • Cisco 2600 series • Cisco 3600 series • Cisco 7100 series • Cisco 7200 series • Cisco 7500 series • Cisco uBR7200 series In Release 12.2(33)SRB, this feature was introduced on the Cisco 7600 Series. The following commands were introduced or modified by this feature: address-family nsap, clear bgp nsap, clear bgp nsap dampening, clear bgp nsap external, clear bgp nsap flap-statistics, clear bgp nsap peer-group, debug bgp nsap, debug bgp nsap dampening, debug bgp nsap updates, neighbor prefix-list, network (BGP and multiprotocol BGP), redistribute (BGP to ISO ISIS), redistribute (ISO ISIS to BGP), show bgp nsap, show bgp nsap community, show bgp nsap community-list, show bgp nsap dampened-paths, show bgp nsap filter-list, show bgp nsap flap-statistics, show bgp nsap inconsistent-as, show bgp nsap neighbors, show bgp nsap paths, show bgp nsap quote-regexp, show bgp nsap regexp, show bgp nsap summary.

Glossary

address family—A group of network protocols that share a common format of network address. Address families are defined by RFC 1700.

AS—autonomous system. An IP term to describe a routing domain that has its own independent routing policy and is administered by a single authority. Equivalent to the OSI term “routing domain.”

BGP—Border Gateway Protocol. Interdomain routing protocol that exchanges reachability information with other BGP systems.

CLNS—Connectionless Network Service. An OSI network-layer protocol.

CMIP—Common Management Information Protocol. In OSI, a network management protocol created and standardized by ISO for the monitoring and control of heterogeneous networks.

DCC—data communications channel.

DCN—data communications network.

ES-IS—End System-to-Intermediate System. OSI protocol that defines how end systems (hosts) announce themselves to intermediate systems (routers).

FTAM—File Transfer, Access, and Management. In OSI, an application-layer protocol developed for network file exchange and management between diverse types of computers.

IGP—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system.

IGRP—Interior Gateway Routing Protocol. A proprietary Cisco protocol, developed to address the issues associated with routing in large, heterogeneous networks.

IS—intermediate system. Routing node in an OSI network.

IS-IS—Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol based on DECnet Phase V routing, where routers exchange routing information based on a single metric, to determine network topology.

ISO—International Organization for Standardization. International organization that is responsible for a wide range of standards, including those relevant to networking. ISO developed the Open System Interconnection (OSI) reference model, a popular networking reference model.

NSAP address—network service access point address. The network address format used by OSI networks.

OSI—Open System Interconnection. International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.

routing domain—The OSI term that is equivalent to autonomous system for BGP.

SDH—Synchronous Digital Hierarchy. Standard that defines a set of rate and format standards that are sent using optical signals over fiber.

SONET—Synchronous Optical Network. High-speed synchronous network specification designed to run on optical fiber.



Note

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

