IPv6 Support on the Cisco ASR 901 Router

This document provides implementation and command reference information for IPv6 features supported on the Cisco ASR 901 router. We strongly recommend that you read this entire document before reading other documents on IPv6 for Cisco IOS software.

Detailed conceptual information about the features supported on the Cisco ASR 901 router, is documented outside of this feature in the Cisco IOS software documentation. For information about the location of this related documentation, see the Feature Information for IPv6 Support on the Cisco ASR 901 Router, on page 42.

Complete configuration information of ASR 901-specific IPv6 features is provided in this document. This information can be found in the How to Configure IPv6 Support on the Cisco ASR 901 Router, on page 8.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for IPv6 Support on the Cisco ASR 901 Router

- Cisco IOS Release 15.2(2)SNG or a later IPv6-supporting release must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- To forward IPv6 traffic using Cisco Express Forwarding (CEF) or distributed CEF, you must configure forwarding of IPv6 unicast datagrams globally on the router by using the ipv6 unicast-routing command, and you must configure an IPv6 address on an interface by using the ipv6 address command.
- You must enable CEF for IPv4 globally on the router by using the ip cef command before enabling Cisco Express Forwarding for IPv6 globally on the router by using the ipv6 cef command.

Restrictions for IPv6 Support on the Cisco ASR 901 Router

- Switch port configuration is not supported.
- The fastethernet interface does not expect more than one IPv6 address.
- The following features are not supported:
  - Tunneling protocols such as IPv4-to-IPv6 or IPv6-to-IPv4
  - IPv6 Policy-Based Routing
  - Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) for IPv6
  - Quality of service (QoS) based on IPv6 addresses
  - IPv6 support of IEEE 1588v2
  - IPv6 support over slower links like time-division multiplexing (TDM) interfaces, Multilink Point-to-Point Protocol (MLPPP), etc
  - IPv6 Access Control Lists (ACLs) was not supported prior to Cisco IOS Release 15.4(2)S.
  - IPv6 over IP and Multiprotocol Label Switching (MPLS)
  - Bidirectional Forwarding Detection for IPv6 (BFDv6) for Intermediate System-to-Intermediate System (IS-IS)
  - IPv6 Virtual Routing and Forwarding (VRF) Lite

Information About IPv6 Support on the Cisco ASR 901 Router

Benefits

IPv6 Support on the Cisco ASR 901 router provides the following benefits:

- Supports state-less auto-configuration of IPv6 addresses.
- Supports the following routing protocols:
  - Static routing
  - Open Shortest Path First (OSPF) version 3
  - Border Gateway Protocol
  - Intermediate System-to-Intermediate System (IS-IS)

Overview of IPv6

IPv6 is the latest version of the Internet Protocol that has a much larger address space and improvements such as a simplified main header and extension headers. The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while providing services such as end-to-end security, quality of service (QoS), and globally unique addresses.

The larger IPv6 address space allows networks to scale and provide global reachability. The simplified IPv6 packet header format handles packets more efficiently. IPv6 supports widely deployed routing protocols such as Routing Information Protocol (RIP), Integrated Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF) for IPv6, and multiprotocol Border Gateway Protocol (BGP). Other available features include stateless autoconfiguration and enhanced support for Mobile IPv6.

IPv6 is being introduced on the Cisco ASR 901 router to support Long Term Evolution (LTE) rollouts that provides high-bandwidth data connection for mobile wireless devices. The IPv6 transport utilizes Switch Virtual Interface (SVI) and Ethernet interfaces. The Cisco ASR 901 router also supports IPv6 addressing on Loopback interfaces.

IPv6 Address Formats

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. Following are two examples of IPv6 addresses:

```
2001:DB8:7654:3210:FEDC:BA98:7654:3210
2001:DB8:0:0:8:800:200C:417A
```

It is common for IPv6 addresses to contain successive hexadecimal fields of zeros. To make IPv6 addresses less complicated, two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). Table 1: Compressed IPv6 Address Formats , on page 3 lists compressed IPv6 address formats.

A double colon may be used as part of the *ipv6-address* argument when consecutive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interface, but only one link-local address.

Note Two colons (::) can be used only once in an IPv6 address to represent the longest successive hexadecimal fields of zeros. The hexadecimal letters in IPv6 addresses are not case-sensitive.

Table 1: Compressed IPv6 Address Formats

IPv6 Address Type	Preferred Format	Compressed Format
Unicast	2001:0:0:0:DB8:800:200C:417A	2001::DB8:800:200C:417A
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

The loopback address listed in Table 1: Compressed IPv6 Address Formats , on page 3 are used by a node to send an IPv6 packet to itself. The loopback address in IPv6 functions the same as the loopback address in IPv4 (127.0.0.1).

Note The IPv6 loopback address cannot be assigned to a physical interface. A packet that has the IPv6 loopback address as its source or destination address must remain within the node that created the packet. IPv6 routers do not forward packets that have the IPv6 loopback address as their source or destination address.

The unspecified address listed in Table 1: Compressed IPv6 Address Formats , on page 3 indicates the absence of an IPv6 address. For example, a newly initialized node on an IPv6 network may use the unspecified address as the source address in its packets until it receives its IPv6 address.

Note The IPv6 unspecified address cannot be assigned to an interface. The unspecified IPv6 addresses must not be used as destination addresses in IPv6 packets or the IPv6 routing header.

An IPv6 address prefix, in the format *ipv6-prefix*/*prefix-length*, can be used to represent bit-wise contiguous blocks of the entire address space. The *ipv6-prefix* must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). For example, 2001:DB8:8086:6502::/32 is a valid IPv6 prefix.

For more information on IPv6 Addressing and Basic Connectivity, see the Implementing IPv6 Addressing and Basic Connectivity chapter of IPv6 Configuration Guide, at the following location:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-addrg-bsc-con.html

IPv6 Addressing and Discovery

The IPv6 addressing and discover consists of static and autoconfiguration of addresses – both global and link local addresses. IPv6 differs from IPv4 in that same interface can have multiple IPv6 addresses assigned to it. The Cisco ASR 901 router supports both IPv4 and multiple IPv6 addresses on the same Loopback and SVI interface. The link-local addresses are automatically generated (if ipv6 enable command is configured) from the MAC-address of the interface as soon as the SVI comes up.

Static Configuration

Static configuration is the manual process of defining an explicit path between two networking devices. The administrator of the network manually enters the IPv6 addresses, subnet masks, gateways, and corresponding MAC addresses for each interface of each router into a table. Static configuration provides more control over the network but it requires more work to maintain the table. The table must be updated every time routes are added or changed. Moreover, the static routes must be manually reconfigured if there is a change in the network topology.

Static configuration provides security and resource efficiency. It uses less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. Static routes created by the static configuration can be redistributed into dynamic routing protocols. However, routes generated by dynamic routing protocols cannot be redistributed into the static routing table.

Static configuration is useful for smaller networks with only one path to an outside network and in providing security for a larger network for certain types of traffic or links to other networks that need more control. In general, most networks use dynamic routing protocols to communicate between networking devices but may have one or two static routes configured for special cases.

Stateless Autoconfiguration

All interfaces on IPv6 nodes must have a link-local address, which is usually automatically configured from the identifier for an interface and the link-local prefix FE80::/10. A link-local address enables a node to communicate with other nodes on the link and can be used to further configure the node.

Nodes can connect to a network and automatically generate global IPv6 addresses without the need for manual configuration or help of a Dynamic Host Configuration Protocol (DHCP) server.

With IPv6, a router on the link advertises in RA messages any global prefixes, and its willingness to function as a default router for the link. RA messages are sent periodically and in response to router solicitation messages, which are sent by hosts at system startup.

A node on the link can automatically configure global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages. The resulting 128-bit IPv6 addresses configured by the node are then subjected to duplicate address detection (DAD) to ensure their uniqueness on the link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also globally unique. Router solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message.

For more information on IPv6 Addressing and Discovery, see the Implementing IPv6 Addressing and Basic Connectivity chapter of IPv6 Configuration Guide, at the following location:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-addrg-bsc-con.html

ICMPv6

Internet Control Message Protocol (ICMP) in IPv6 functions the same as ICMP in IPv4. ICMP generates error messages such as ICMP destination unreachable messages, and informational messages such as ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process, path MTU discovery, and the Multicast Listener Discovery (MLD) protocol for IPv6.

For more information on ICMPv6, see the Implementing IPv6 Addressing and Basic Connectivity chapter of IPv6 Configuration Guide, at the following location:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-addrg-bsc-con.html

IPv6 Duplicate Address Detection

During the stateless autoconfiguration process, duplicate address detection (DAD) verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). DAD is first performed first on the new link-local address. When the link local address is verified as unique, then DAD is performed on the remaining IPv6 unicast addresses on the interface.

When a duplicate address is identified, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message is issued. If the duplicate address is a global address of the interface, the address is not used and an error message is issued. However, all configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMPv6 messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and keep track of neighboring routers.

Neighbor solicitation messages (ICMPv6 Type 135) are sent on the local link by nodes attempting to discover the link-layer addresses of other nodes on the local link. The neighbor solicitation message is sent to the solicited-node multicast address.The source address in the neighbor solicitation message is the IPv6 address of the node sending the neighbor solicitation message. The neighbor solicitation message also includes the link-layer address of the source node.

After receiving a neighbor solicitation message, the destination node replies by sending a neighbor advertisement message (ICPMv6 Type 136) on the local link. The source address in the neighbor advertisement message is the IPv6 address of the node sending the neighbor advertisement message; the destination address is the IPv6 address of the node that sent the neighbor solicitation message. The data portion of the neighbor advertisement message includes the link-layer address of the node sending the neighbor advertisement message.

After the source node receives the neighbor advertisement, the source node and destination node communicate with each other.

For more information on IPv6 Neighbor Discovery, see the Implementing IPv6 Addressing and Basic Connectivity chapter of IPv6 Configuration Guide, at the following location:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-addrg-bsc-con.html

IPv4 and IPv6 Dual-Stack on an Interface

A dual stack means that IPv4 and IPv6 addresses coexist on the same platform and support hosts of both types. This method is a way to transition from IPv4 to IPv6 with coexistence (IPv4 and IPv6) as a first step.

The Cisco ASR 901 router supports the configuration of both IPv6 and IPv4 on an interface. You do not need to enter any specific commands to do so; simply enter the IPv4 configuration commands and IPv6 configuration commands as you normally would. Make sure you configure the default route for both IPv4 and IPv6.

Routing Protocols

The Cisco ASR 901 router supports widely deployed routing protocols such as IS-IS, OSPFv3, and multiprotocol BGP.

IS-IS Enhancements for IPv6

IS-IS in IPv6 functions the same as in IPv4 and offers many of the same benefits as IS-IS in IPv4. IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and OSI routes. Extensions to the IS-IS command-line interface (CLI) allow configuration of IPv6-specific parameters. IPv6 IS-IS extends the address families supported by IS-IS to include IPv6, in addition to OSI and IPv4.

For more information on IS-IS Enhancements for IPv6, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-is-is.html

OSPFv3 for IPv6

OSPF is a routing protocol for IP. It is a link-state protocol. A link-state protocol makes its routing decisions based on the states of the links that connect source and destination machines. The state of a link is a description

of that interface, and its relationship to its neighboring networking devices. The interface information includes the IPv6 prefix of the interface, the network mask, the type of network it is connected to, the devices connected to that network, and so on. This information is propagated in various type of link-state advertisements (LSAs).

For more information on OSPFv3 for IPv6, refer the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-ospf.html

Multiprotocol BGP Extensions for IPv6

Multiprotocol BGP is the supported exterior gateway protocol (EGP) for IPv6. Multiprotocol BGP extensions for IPv6 support many of the same features and functionality as IPv4 BGP. IPv6 enhancements to multiprotocol BGP include support for an IPv6 address family and network layer reachability information (NLRI) and next hop (the next router in the path to the destination) attributes that use IPv6 addresses.

For more information on Multiprotocol BGP Extensions for IPv6, refer the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-mptcl-bgp.html

Bidirectional Forwarding Detection for IPv6

The BFDv6 is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. BFDv6 provides IPv6 support by accommodating IPv6 addresses and provides the ability to create BFDv6 sessions.

For more information on Bidirectional Forwarding Detection for IPv6, refer the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-bfd.html

QoS for IPv6

The Cisco ASR 901 router support of QoS features for IPv6 environments include ingress packet classification, policing, marking on Ethernet interfaces. It also supports egress packet classification, marking, scheduling, per interface and per qos-group shaping, Low Latency Queuing (LLQ), and weighted random early detection (WRED) on GigabitEthernet interfaces.

Note Queuing, shaping, scheduling and LLQ is not supported on the ingress path for the Ethernet interfaces. Policing is not supported on the egress path for GigabitEthernet interfaces.

The QoS implementation for IPv6 environment in the Cisco ASR router is the same as that of IPv4. For more information on Configuring QoS on the Cisco ASR 901 router, refer the following link:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/qos.html

For additional information on Implementing QoS for IPv6, refer the following link:
http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-qos.html

How to Configure IPv6 Support on the Cisco ASR 901 Router

Configuring IPv6 Addressing and Enabling IPv6 Routing

Perform this task to assign IPv6 addresses to individual router interfaces and enable IPv6 traffic forwarding globally on the router. By default, IPv6 addresses are not configured, and IPv6 routing is disabled.

Procedure

	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** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address/prefix-length* {**eui-64 | link-local | anycast** } **Example:** `Router(config-if)# ipv6 address 2001:DB8:FFFF::2/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface. • **eui-64**—Specifies the global IPv6 addresses with an interface identifier (ID) in the low-order 64 bits of the IPv6 address. Only the 64-bit network prefix for the address needs to be specified; the last 64 bits are automatically computed from the interface ID. • **link-local**—Specifies the link-local address on the interface that is used instead of the link-local address that is automatically configured when IPv6 is enabled on the interface. • **anycast**—Specifies an IPv6 anycast address.
Step 5	**ipv6 enable** **Example:**	Enables IPv6 on the interface.

	Command or Action	Purpose
	`Router(config-if)# ipv6 enable`	
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns the router to global configuration mode.
Step 7	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 8	**ipv6 cef** **Example:** `Router(config)# ipv6 cef`	Enables Cisco Express Forwarding (CEF) globally on the router.

Configuring a Static IPv6 Route

Procedure

	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	**ipv6 route** {*ipv6-prefix* | *prefix-length ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**tag** *tag*] **Example:** `Router(config)# ipv6 route 2001::/64 5::5 100`	Configures a static default IPv6 route. • *ipv6-prefix*—The IPv6 network that is the destination of the static route. This could also be a host name when static host routes are configured. • *prefix-length*—The length of the IPv6 prefix. • *ipv6-address*—(Optional) The IPv6 address of the next hop that can be used to reach the specified network. • *interface-type*—Interface type. • *interface-number*—Interface number.

	Command or Action	Purpose
		• *administrative-distance*—(Optional) An administrative distance. The default value is 1, which gives static routes precedence over any other type of route except connected routes. • *administrative-multicast-distance*—(Optional) The distance used when selecting this route for multicast Reverse Path Forwarding (RPF). • **unicast**—(Optional) Specifies a route that must not be used in multicast RPF selection. • **multicast**—(Optional) Specifies a route that must not be populated in the unicast Routing Information Base (RIB). • *tag*—(Optional) Tag value that is used as a "match" value for controlling redistribution via route maps.

Enabling Stateless Auto-Configuration

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# Interface fastethernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 address autoconfig** **Example:** `Router(config-if)# ipv6 address autoconfig`	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.

Implementing IPv6 on VLAN Interfaces

Perform the tasks given below to enable IPv6 on VLAN interfaces. By default, IPv6 is disabled on an interface.

Note For information on how to create a VLAN interface, see the Configuring Ethernet Virtual Connections document at the following location:
http://www.cisco.com/en/US/partner/docs/wireless/asr_901/Configuration/Guide/swevc.html

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# Interface vlan 40`	Specifies an interface type and number, and places the router in interface configuration mode. farce

Step 4	Do one of the following:
	• **ipv6 enable**
	• **ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}
	Example:
	`Router(config-if)# ipv6 enable`
	`or`
	Example:
	`Router(config-if)# ipv6 address 2000::1/64`
		Configures IPv6 on the VLAN interface. Though both the commands automatically configure the link local address (LLA) on the interface, the **ipv6 address** command additionally configures an ipv6 address on the interface.
		• *ipv6-address*—The IPv6 address to be used.
		• *prefix-length*—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
		• *prefix-name*—A general prefix, which specifies the leading bits of the network to be configured on the interface.
		• *sub-bits*—The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument.

Implementing IPv6 Addressing on Loopback Interfaces

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# Interface loopback 0`	Specifies an interface type and number, and places the router in interface configuration mode.

Step 4	Do one of the following:
	• **ipv6 enable**
	• **ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}
	Example:
	`Router(config-if)# ipv6 enable`
	`or`
	Example:
	`Router(config-if)# ipv6 address 2000::1/64`
		Configures IPv6 on the Loopback interface. Though both the commands automatically configure the link local address (LLA) on the interface, the **ipv6 address** command additionally configures an ipv6 address on the interface.
		• *ipv6-address*—The IPv6 address to be used.
		• *prefix-length*—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
		• *prefix-name*—A general prefix, which specifies the leading bits of the network to be configured on the interface.
		• *sub-bits*—The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument.

Configuring ICMPv6 Rate Limiting

Procedure

	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	**ipv6 icmp error-interval** *interval* **Example:** `Router(config)# ipv6 icmp error-interval 1200`	Configures the interval for IPv6 ICMP error messages. • *interval*—Specifies the interval between tokens, in milliseconds, being added to the bucket. The valid range is from 0 to 2147483647.

Configuring IPv6 Duplicate Address Detection

Procedure

	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** *type number* **Example:** `Router(config)# Interface Vlan 40`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 nd dad attempts** *value* **Example:** `Router(config)ipv6 nd dad attempts 5`	Configures the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is

	Command or Action	Purpose
		performed on the unicast IPv6 addresses of the interface.

Configuring IPv6 Neighbor Discovery

Procedure

	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 type number** **Example:** `Router(config)# Interface fastEthernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 nd {advertisement-interval | autoconfig | cache | dad | managed-config-flag | na | ns-interval | nud | other-config-flag | prefix | ra | reachable-time | router-preference}** **Example:** `Router(config-if)# ipv6 nd autoconfig`	Configures a Neighbor Discovery on a specified interface on the router. • **advertisement-interval**—Sends an advertisement interval option in router advertisements (RAs). • **autoconfig**—Automatic configuration. • **cache**—Cache entry. • **dad**—Duplicate Address Detection. • **managed-config-flag**—Hosts should use DHCP for address config. • **na**—Neighbor advertisement control. Configures ND to extract an entry from an unsolicited NA. • **ns-interval**— Sets the advertised NS retransmission interval. • **nud** —Configures the number of times neighbor unreachability detection (NUD) resends neighbor solicitations (NSs). • **other-config-flag**—Hosts should use DHCP for non-address config.

	Command or Action	Purpose
		• **prefix**—Configures which IPv6 prefixes are included in IPv6 ND router advertisements. • **ra**—Router advertisement control. • **reachable-time**—Sets the advertised reachability time. • **router-preference**—Sets the default router preference value.

Configuring IPv6 and IPv4 Dual-Stack on the Same VLAN

Before you begin

You should enable IPv6 routing before proceeding with this task. See Configuring IPv6 Addressing and Enabling IPv6 Routing, on page 8.

Procedure

	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 type number** **Example:** `Router(config)# interface fastEthernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config)# ip address 192.168.99.1 255.255.255.0`	Configures an IPv4 address on the interface.
Step 5	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*} **Example:** `Router(config)# ipv6 address 2000::1/64`	Configures IPv6 address on the interface. • *ipv6-address*—The IPv6 address to be used. • *prefix-length*—The length of the IPv6 prefix. A decimal value that indicates how

	Command or Action	Purpose
		many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. • *prefix-name*—A general prefix, which specifies the leading bits of the network to be configured on the interface. • *sub-bits*—The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument.
Step 6	**ipv6 enable** **Example:** `Router(config)# ipv6 enable`	Enables IPv6 address on the interface.

Configuring OSPFv3 for IPv6

Procedure

	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 type number** **Example:** `Router(config)# interface fastEthernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 ospf** *process-id* **area** *area-id* **[instance** *instance-id***]** **Example:** `Router(config-if)# ipv6 ospf 1 area 0`	Enables OSPFv3 on an interface. • *process-id*—Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPFv3 routing process. • *area-id*—Area that is to be associated with the OSPFv3 interface.

	Command or Action	Purpose
		• *instance-id*—(Optional) Instance identifier.

Configuring IS-IS for IPv6

Procedure

	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 area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode. • *area-tag*—Name for a routing process.
Step 4	**net** *network-entity-title* **Example:** `Router(config-router)# net 49.0001.0000.0000.000c.00`	Configures an IS-IS network entity title (NET) for the routing process. • *network-entity-title*—The network-entity-title argument defines the area addresses for the IS-IS area and the system ID of the router.
Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode and enters global configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface fastEthernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 7	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*} **Example:** `Router(config-if)# ipv6 address 2001:DB8::3/64`	Specifies the IPv6 network assigned to the interface and enables IPv6 processing on the interface. • *ipv6-address*—The IPv6 address to be used.

	Command or Action	Purpose
		• *prefix-length*—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. • *prefix-name*—A general prefix, which specifies the leading bits of the network to be configured on the interface. • *sub-bits*—The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument.
Step 8	**ipv6 router isis** *area-name* **Example:** `Router(config-if)# ipv6 router isis area2`	Enables the specified IPv6 IS-IS routing process on an interface. • *area-name*—Meaningful name for a routing process. If a name is not specified, a null name is assumed and the process is referenced with a null name. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. Required for multiarea IS-IS configuration. Each area in a multiarea configuration should have a non-null area name to facilitate identification of the area. Optional for conventional IS-IS configuration.

Configuring Multiprotocol-BGP for IPv6

Perform this task to configure an IPv6 BGP routing process and an optional BGP router ID for a BGP-speaking router.

Procedure

	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.

	Command or Action	Purpose
Step 3	**router bgp** *as-number* **Example:** `Router(config)# router bgp 65000`	Configures a BGP routing process, and enters router configuration mode for the specified routing process. • *as-number*—Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. The range is from 1 to 65535.
Step 4	**no bgp default ipv4-unicast** **Example:** `Router(config-router)# no bgp default ipv4-unicast`	Disables the IPv4 unicast address family for the BGP routing process specified in the previous step.
Step 5	**bgp router-id** *ip-address* **Example:** `Router(config-router)# bgp router-id 192.168.99.70`	(Optional) Configures a fixed 32-bit router ID as the identifier of the local router running BGP.

Configuring BFD for IPv6

Perform the tasks given below to configure Bidirectional Forwarding Detection (BFD) for IPv6:

Specifying a Static BFDv6 Neighbor

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ipv6 route static bfd [vrf** *vrf-name***]** *interface-type interface-number ipv6-address* **[unassociated]** **Example:**	Specifies static route IPv6 BFDv6 neighbors. • *vrf-name*—(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes are specified. • *interface-type*—Interface type.

	Command or Action	Purpose
	`Router(config)# ipv6 route static bfd vlan 4000 2001::1`	• *interface-number*—SVI name. • *ipv6-address*—IPv6 address of the neighbor. • **unassociated**—(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.

Associating an IPv6 Static Route with a BFDv6 Neighbor

IPv6 static routes are automatically associated with a static BFDv6 neighbor. A static neighbor is associated with a BFDv6 neighbor if the static next-hop explicitly matches the BFDv6 neighbor.

Procedure

	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	**ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**] **Example:** `Router(config)# ipv6 route static bfd vlan 4000 2001::1`	Specifies static route IPv6 BFDv6 neighbors. • *vrf-name*—(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes are specified. • *interface-type*—Interface type. • *interface-number*—SVI name. • *ipv6-address*—IPv6 address of the neighbor. • **unassociated**—(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.
Step 4	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-type* [*interface-number ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance*] [**unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] **Example:**	Establishes static IPv6 routes. • *vrf-name*—(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes are specified. • *ipv6-prefix*—The IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.

	Command or Action	Purpose
	`Router(config)# ipv6 route 2001:DB8::/64 vlan 4000 2001::1`	• *ipv6-address*—The IPv6 address of the next hop that can be used to reach the specified network. • *interface-type*—Interface type. • *interface-number*—SVI name. • **nexthop-vrf**—(Optional) Indicator that the next hop is a VRF. • *vrf-name1*—(Optional) Name of the next-hop VRF. • **default**—(Optional) Indicator that the next hop is the default. • *administrative-distance*—(Optional) An administrative distance. The default value is 1, which gives static routes precedence over any other type of route except connected routes. • *administrative-multicast-distance*—(Optional) The distance used when selecting this route for multicast Reverse Path Forwarding (RPF). • **unicast**—(Optional) Specifies a route that must not be used in multicast RPF selection. • **multicast**—(Optional) Specifies a route that must not be populated in the unicast Routing Information Base (RIB). • *next-hop-address*—(Optional) Address of the next hop that can be used to reach the specified network. • **tag** *tag*—(Optional) Tag value that is used as a “match” value for controlling redistribution via route maps.

Configuring BFDv6 and OSPFv3

This section describes the procedures for configuring BFD support for OSPFv3, so that OSPFv3 is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD.

There are two methods for enabling BFD support for OSPFv3:

- You can enable BFD for all of the interfaces for which OSPFv3 is routing by using the **bfd all-interfaces** command in router configuration mode.
- You can enable BFD for a subset of the interfaces for which OSPFv3 is routing by using the **ipv6 ospf bfd** command in interface configuration mode.

Before you begin

- OSPFv3 must be running on all participating routers.

- The baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured.

Procedure

	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	**ipv6 router ospf** *process-id* **Example:** `Router(config)# ipv6 router ospf 2`	Configures an OSPFv3 routing process. • *process-id*—Internal identification. It is locally assigned and can be a positive integer from 1 to 65535. The number used here is the number assigned administratively when enabling the OSPF for IPv6 routing process.
Step 4	**bfd all-interfaces** **Example:** `Router(config-rtr)# bfd all-interfaces`	Enables BFD for all interfaces participating in the routing process
Step 5	**end** **Example:** `Router(config-rtr)# end`	Enter this command twice to go to privileged EXEC mode.

Configuring BFDv6 for BGP

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**router bgp** *as-tag* **Example:** `Router(config)# router bgp 4500`	Specifies a BGP process and enter router configuration mode. • *as-tag*—Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. The range is from 1 to 65535.
Step 4	**neighbor** *ip-address* **fall-over bfd** **Example:** `Router(config-router)# neighbor 10.0.0.1 fall-over bfd`	Enables support for BFD failover. • *ip-address*—IPv4 or IPv6 address of a BGP neighbor. • **bfd**—Enables BFD protocol support for fallover.
Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Implementing QoS for IPv6

The QoS implementation for IPv6 environment in the Cisco ASR router is the same as that of IPv4. For configuration information on Configuring QoS on the Cisco ASR 901 router, refer the following link:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/qos.html

For additional information on Implementing QoS for IPv6, refer the following link:
http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-qos.html

Verifying the Configuration of IPv6 Support on the Cisco ASR 901 Router

This section describes how to use the **show** commands to verify the configuration and operation of the IPv6 Support feature on the Cisco ASR 901 router, and it contains the following topics:

Verifying IPv6 Addressing Routing

To verify the IPv6 Addressing Routing information, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface
Vlan40 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    2011:8:8:3::4, subnet is 2011:8:8:3::/64
  Joined group address(es):
    FF02::1
```

```
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

Verifying a Static IPv6 Route

To verify the static IPv6 route information, use the **show ipv6 route** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   22::/64 [0/0]
     via Vlan111, directly connected
L   22::22/128 [0/0]
     via Vlan111, receive
C   33::/64 [0/0]
     via Vlan111, directly connected
L   33::33/128 [0/0]
     via Vlan111, receive
I1  454::/96 [115/20]
     via FE80::4255:39FF:FE89:3F71, Vlan2020
```

Verifying a Stateless Auto-Configuration

To verify the autoconfigured IPv6 address and its state, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface loopback 0
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

Verifying IPv6 Implementation on VLAN Interfaces

To verify the IPv6 implementation on VLAN interfaces, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface vlan40
Vlan40 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    2011:8:8:3::4, subnet is 2011:8:8:3::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Verifying IPv6 Implementation on Loopback Interfaces

To verify the IPv6 implementation on loopback interfaces, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface loopback0
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

Verifying ICMPv6 Configuration

To verify the ICMPv6 configuration information, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface
Vlan40 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    2011:8:8:3::4, subnet is 2011:8:8:3::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
```

```
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

To verify the ICMPv6 statistics, use the **show ipv6 traffic** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 traffic
IPv6 statistics:
        Rcvd:  8 total, 0 local destination
               0 source-routed, 0 truncated
               0 format errors, 0 hop count exceeded
               0 bad header, 0 unknown option, 0 bad source
               0 unknown protocol, 0 not a router
               0 fragments, 0 total reassembled
               0 reassembly timeouts, 0 reassembly failures
        Sent:  870 generated, 0 forwarded
               0 fragmented into 0 fragments, 0 failed
               0 encapsulation failed, 0 no route, 0 too big
               0 RPF drops, 0 RPF suppressed drops
        Mcast: 8 received, 855 sent
ICMP statistics:
        Rcvd: 8 input, 0 checksum errors, 0 too short
              0 unknown info type, 0 unknown error type
              unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
                       0 sa policy, 0 reject route
              parameter: 0 error, 0 header, 0 option
              0 hopcount expired, 0 reassembly timeout,0 too big
              0 echo request, 0 echo reply
              0 group query, 0 group report, 0 group reduce
              0 router solicit, 0 router advert, 0 redirects
              0 neighbor solicit, 0 neighbor advert
        Sent: 129 output, 0 rate-limited
              unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
                       0 sa policy, 0 reject route
              parameter: 0 error, 0 header, 0 option
              0 hopcount expired, 0 reassembly timeout,0 too big
              0 echo request, 0 echo reply
              0 group query, 0 group report, 0 group reduce
              0 router solicit, 50 router advert, 0 redirects
              8 neighbor solicit, 8 neighbor advert
UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output
TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Verifying IPv6 Duplicate Address Detection Configuration

To verify the IPv6 Duplicate Address Detection configuration information, use the **show running configuration** command or the **show ipv6 interface command** in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface
Vlan40 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    2011:8:8:3::4, subnet is 2011:8:8:3::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

Verifying IPv6 Neighbor Discovery Configuration

To verify the IPv6 neighbor discovery configuration, use the **show ipv6 neighbors** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 neighbors detail
IPv6 Address                              TRLV Age Link-layer Addr State Interface
2001:103::2                                 0    0 001e.4a97.05bb  REACH Vl103
2001:101::2                                 0    0 001e.4a97.05bb  REACH Vl101
2001:300::2                                 0   72 001e.4a97.05bb  STALE Vl300
2001:10::2                                  0    0 001e.4a97.05bb  REACH Vl10
```

```
FE80::200:1FF:FE97:41FE                     0   65 0000.0197.41fe  STALE Vl90
FE80::21E:4AFF:FE97:5BB                     0   25 001e.4a97.05bb  STALE Vl101
FE80::21E:4AFF:FE97:5BB                     0    0 001e.4a97.05bb  REACH Vl10
FE80::21E:4AFF:FE97:5BB                     0    0 001e.4a97.05bb  REACH Vl170
FE80::21E:4AFF:FE97:5BB                     0    0 001e.4a97.05bb  STALE Vl160
2001:170::2                                 0    0 001e.4a97.05bb  REACH Vl170
2001:180::2                                 0    0 001e.4a97.05bb  REACH Vl180
2001:190::2                                 0    0 001e.4a97.05bb  REACH Vl190
```

Verifying IPv6 and IPv4 Dual-Stack Configuration

To verify the IPv6 and IPv4 dual-stack configuration, use the **show ipv6 interface or show ip interface** commands in privileged EXEC mode, as shown in the examples.

```
Router# show ipv6 interface loopback0
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
Router# show ip interface
GigabitEthernet0/0 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/1 is administratively down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/2 is up, line protocol is up
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/3 is up, line protocol is up
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/4 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/5 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/6 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
```

```
GigabitEthernet0/7 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/8 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/9 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/10 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/11 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
FastEthernet0/0 is administratively down, line protocol is down
  Internet protocol processing disabled
Vlan1 is down, line protocol is down
  Internet protocol processing disabled
Vlan40 is up, line protocol is up
  Internet protocol processing disabled
Loopback0 is up, line protocol is up
  Internet protocol processing disabled
```

Verifying OSPFv3 for IPv6 Configuration

To verify the OSPF for IPv6 configuration, use the **show ipv6 ospf** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 ospf
 Routing Process "ospfv3 10" with ID 4.4.4.4
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 RFC1583 compatibility enabled
    Area 34
        Number of interfaces in this area is 2
        SPF algorithm executed 5 times
        Number of LSA 3. Checksum Sum 0x01F6C1
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Verifying IS-IS for IPv6 Configuration

To verify the IPv6 Addressing Routing information, use the **show isis ipv6 rib** command in privileged EXEC mode, as shown in the example.

```
Router# show isis ipv6 rib
IS-IS IPv6 process area2, local RIB
```

Verifying Multiprotocol-BGP for IPv6 Configuration

To verify the IPv6 Addressing Routing information, use the **show bgp ipv6** command in privileged EXEC mode, as shown in the examples.

```
Router# show bgp ipv6 unicast summary
BGP router identifier 9.9.9.9, local AS number 5500
BGP table version is 25, main routing table version 25
15 network entries using 2580 bytes of memory
53 path entries using 4664 bytes of memory
3/3 BGP path/bestpath attribute entries using 384 bytes of memory
1 BGP AS-PATH entries using 24 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 using 7652 total bytes of memory
BGP activity 43/2 prefixes, 134/46 paths, scan interval 60 secs
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:10::2      4         6500       0       0        1    0    0 00:22:30 Idle
2001:101::2     4         6500      87      84       25    0    0 01:09:28        8
2001:103::2     4         6500      84      83       25    0    0 01:09:34        8
2001:170::2     4         6500      88      82       25    0    0 01:09:33        8
2001:180::2     4         6500      87      84       25    0    0 01:09:29        8
2001:190::2     4         6500      89      83       25    0    0 01:09:34        8
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:300::2     4         6500       0       0        1    0    0 01:09:23 Idle
FE80::21E:4AFF:FE97:5BB%Vlan160
                4         6500      82      82       25    0    0 01:09:25        5
Router# show bgp ipv6 unicast neighbors 2001:101::2
BGP neighbor is 2001:101::2,  remote AS 6500, external link
 Fall over configured for session
 BFD is configured.  Using BFD to detect fast fallover
  BGP version 4, remote router ID 14.14.14.14
  BGP state = Established, up for 01:09:48
  Last read 00:00:10, last write 00:00:23, hold time is 180, keepalive interval is 60 seconds

  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv6 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                8          9
    Keepalives:            75         76
    Route Refresh:          0          0
```

```
    Total:                 84         88
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  Session: 2001:101::2
  BGP table version 25, neighbor version 25/0
  Output queue size : 0
  Index 1, Advertise bit 0
  1 update-group member
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:             15          8 (Consumes 704 bytes)
    Prefixes Total:               16         10
    Implicit Withdraw:             0          0
    Explicit Withdraw:             1          2
    Used as bestpath:            n/a          3
    Used as multipath:           n/a          0
                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    AS_PATH loop:                      n/a          4
    Invalid Path:                        2        n/a
    Total:                               2          4
  Number of NLRIs in the update sent: max 7, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
  Refresh Epoch: 2
  Last Sent Refresh Start-of-rib: never
  Last Sent Refresh End-of-rib: never
  Last Received Refresh Start-of-rib: 01:09:48
  Last Received Refresh End-of-rib: 01:09:48
  Refresh-In took 0 seconds
                                     Sent       Rcvd
        Refresh activity:            ----       ----
          Refresh Start-of-RIB        0          1
          Refresh End-of-RIB          0          1
  Address tracking is disabled
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Mininum incoming TTL 0, Outgoing TTL 1
Local host: 2001:101::1, Local port: 57438
Foreign host: 2001:101::2, Foreign port: 179
Connection tableid (VRF): 0
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x4853F8):
Timer          Starts    Wakeups            Next
Retrans            83          0             0x0
TimeWait            0          0             0x0
AckHold            83         81             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger        10940      10939        0x485427
DeadWait            0          0             0x0
Linger              0          0             0x0
iss:  338855921  snduna:  338858128  sndnxt:  338858128     sndwnd:  15636
irs:  816933509  rcvnxt:  816935775  rcvwnd:      15571  delrcvwnd:    813
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: none
```

```
Option Flags: higher precendence, nagle, path mtu capable
Datagrams (max data segment is 1440 bytes):
Rcvd: 163 (out of order: 0), with data: 86, total data bytes: 2265
Sent: 167 (retransmit: 0 fastretransmit: 0),with data: 167, total data bytes: 8894
```

Verifying BFD for IPv6 Configuration

To verify the IPv6 Addressing Routing information, use the **show bfd neighbors** command in privileged EXEC mode, as shown in the example.

```
Router# show bfd neighbors
IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
101.101.101.2                           6/5          Up        Up        Vl101
103.103.103.2                           7/6          Up        Up        Vl103
150.150.150.2                           2/1          Up        Up        Vl150
IPv6 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
2001:10::2                             16/14         Up        Up        Vl10
2001:101::2                            12/11         Up        Up        Vl101
2001:103::2                             3/2          Up        Up        Vl103
2001:170::2                             8/7          Up        Up        Vl170
2001:180::2                            11/10         Up        Up        Vl180
2001:190::2                             4/3          Up        Up        Vl190
FE80::21E:4AFF:FE97:5BB                13/12         Up        Up        Vl160
CE1-2009#
```

Verifying BFDv6 and OSPFv3 Configuration

To verify the BFDv6 and OSPFv3 configuration, use the **show bfd neighbors or the show ipv6 ospf** command in privileged EXEC mode, as shown in the examples.

```
Router# show bfd neighbors
IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
101.101.101.2                           6/5          Up        Up        Vl101
103.103.103.2                           7/6          Up        Up        Vl103
150.150.150.2                           2/1          Up        Up        Vl150
IPv6 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
2001:10::2                             16/14         Up        Up        Vl10
2001:101::2                            12/11         Up        Up        Vl101
2001:103::2                             3/2          Up        Up        Vl103
2001:170::2                             8/7          Up        Up        Vl170
2001:180::2                            11/10         Up        Up        Vl180
2001:190::2                             4/3          Up        Up        Vl190
FE80::21E:4AFF:FE97:5BB                13/12         Up        Up        Vl160
Router# show ipv6 ospf
 Routing Process "ospfv3 10" with ID 4.4.4.4
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

```
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 RFC1583 compatibility enabled
    Area 34
        Number of interfaces in this area is 2
        SPF algorithm executed 11 times
        Number of LSA 3. Checksum Sum 0x01D6D1
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Verifying BFDv6 for BGP Configuration

To verify the BFDv6 for BGP configuration, use the **show bfd neighbors** command in privileged EXEC mode, as shown in the example.

```
Router# show bfd neighbors
IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
101.101.101.2                           6/5          Up        Up        Vl101
103.103.103.2                           7/6          Up        Up        Vl103
150.150.150.2                           2/1          Up        Up        Vl150
IPv6 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
2001:10::2                             16/14         Up        Up        Vl10
2001:101::2                            12/11         Up        Up        Vl101
2001:103::2                             3/2          Up        Up        Vl103
2001:170::2                             8/7          Up        Up        Vl170
2001:180::2                            11/10         Up        Up        Vl180
2001:190::2                             4/3          Up        Up        Vl190
FE80::21E:4AFF:FE97:5BB                13/12         Up        Up        Vl160
CE1-2009#
```

Configuration Examples for IPv6 Support on the Cisco ASR 901 Router

This section provides sample configuration examples for IPv6 Support on the Cisco ASR 901 router feature.

Example: IPv6 Addressing on VLAN Interfaces

The following is a sample configuration of IPv6 addressing on VLAN interfaces.

```
!
interface Vlan2020
 ip address 4.5.6.7 255.255.255.0
 ipv6 address FE80::3 link-local
 ipv6 address 3333::3335/64
 ipv6 address 4400::/64 anycast
 ipv6 address autoconfig
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

Example: IPv6 Addressing on Loopback Interfaces

The following is a sample configuration of IPv6 addressing on Loopback interfaces.

```
!
interface Loopback100
 ip address 170.0.0.201 255.255.255.0
!
interface Loopback555
 no ip address
 ipv6 address 22::22/64
 ipv6 address 555::554/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

Example: Customizing ICMPv6

The following is a sample configuration of customizing ICMPv6.

```
!

  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
!
```

Example: Configuring IPv6 Duplicate Address Detection

The following is a sample configuration of IPv6 duplicate address detection.

```
!

  ND DAD is enabled, number of DAD attempts: 1
!Duplicate address detection information is given above.
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
!
```

Example: Configuring IPv6 Neighborhood Discovery

The following is a sample configuration of IPv6 neighborhood discovery.

```
!
interface Vlan111
 no ip address
 ipv6 address 22::22/64
 ipv6 address 33::33/64
ipv6 address autoconfig
ipv6 nd autoconfig prefix
```

```
!Neighborhood discovery information is given above.
 ipv6 enable
```

Example: Enabling IPv6 Stateless Address Autoconfiguration

The following is a sample configuration of IPv6 stateless address autoconfiguration.

```
!
interface Vlan111
 no ip address
 ipv6 address 22::22/64
 ipv6 address 33::33/64
ipv6 address autoconfig
!IPv6 address autoconfiguration details are given above.
ipv6 nd autoconfig prefix
 ipv6 enable
!
```

Example: Configuring the IPv4 and IPv6 Dual-Stack

The following is a sample configuration of IPv4 and IPv6 dual-stack.

```
!
interface Vlan222
 ip address 22.22.22.22 255.255.255.0
 ipv6 address 99::99/64
!IPv4 and IPv6 dual-stack information is given above.
 ipv6 enable
!
```

Example: Configuring IPv6 Static Routing

The following is a sample configuration of IPv6 static routing between two Cisco ASR 901 routers.

Router-1

```
ipv6 route 555::/64 Vlan2020
```

Router-2

```
interface Loopback555
 no ip address
 ipv6 address 22::22/64
 ipv6 address 555::554/64
 ipv6 enable
 ipv6 ospf 1 area 0
```

Example: Configuring BFD and Static Routing for IPv6

The following is a sample configuration of bidirectional forwarding detection and static routing for IPv6.

```
!
```

```
ipv6 route static bfd vlan 4000 2001::1
ipv6 route 2001:DB8::/64 vlan 4000 2001::1
interface vlan 4000
ipv6 add 2001::2/64
bfd interval 50 min_rx 50 multiplier 3
```

Example: Configuring OSPFv3 for IPv6

The following is a sample configuration of OSPFv3 for IPv6.

Router-1

```
!
interface Loopback20202
 no ip address
 ipv6 address 4444::4444/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
 ipv6 router ospf 1
 router-id 1.1.1.1
 area 0 range 4444::/48
!
```

Router-2

```
!
interface Loopback30303
 no ip address
 ipv6 address 4444::4443/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
 ipv6 router ospf 1
 router-id 3.3.3.3
 area 0 range 4444::/48
!
```

Example: Configuring BFD and OSPFv3 for IPv6

The following is a sample configuration of bidirectional forwarding detection support for OSPFv3 on one or more OSPFv3 Interfaces:

```
!
!
ipv6 router ospf 1
router-id 1.1.1.1
interface vlan 4000
ipv6 add 2001::2/64
ipv6 ospf 1 area 0
 ipv6 ospf bfd
bfd interval 50 min_rx 50 multiplier 3
!
```

The following is a sample configuration of bidirectional forwarding detection support for OSPFv3 on all interfaces:

```
ipv6 router ospf 1
router-id 1.1.1.1
bfd all-interfaces
interface vlan 4000
ipv6 add 2001::2/64
ipv6 ospf 1 area 0
bfd interval 50 min_rx 50 multiplier 3
```

Example: Configuring IS-IS for IPv6

The following is a sample configuration of IS-IS for IPv6.

Router-1

```
!
interface Loopback20202
 no ip address
 ipv6 address 565::565/96
 ipv6 address 4444::4444/64
 ipv6 enable
 ipv6 router isis alpha
 !
router isis alpha
 net 49.1111.2222.3333.4444.00
!
```

Router-2

```
!
interface Loopback30303
 no ip address
 ipv6 address 454::454/96
 ipv6 address 4444::4443/64
 ipv6 enable
 ipv6 router isis alpha
!
router isis alpha
 net 49.1111.2220.3330.4440.00
!
```

Example: Configuring Multiprotocol-BGP for IPv6

The following is a sample configuration of multiprotocol-BGP for IPv6.

Router-1

```
--------
ipv6 unicast-routing
!Enables forwarding of IPv6 packets.
ipv6 cef
interface Loopback10
 no ip address
 ipv6 address 2010:AB8:2::/48
 ipv6 enable
!
```

```
interface Loopback20
 no ip address
 ipv6 address 2010:AB8:3::/48
 ipv6 enable
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:AB8:0:2::/64 eui-64
 ipv6 enable
!
router bgp 1
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
!Without configuring "no bgp default ipv4-unicast" only IPv4 will be advertised.
 bgp log-neighbor-changes
 neighbor 2010:AB8:0:2:C601:10FF:FE58:0 remote-as 2
 !
 address-family ipv6
  neighbor 2010:AB8:0:2:C601:10FF:FE58:0 activate
  network 2010:AB8:2::/48
  network 2010:AB8:3::/48
 exit-address-family
!
```

Router-2

```
ipv6 unicast-routing
ipv6 cef
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:AB8:0:2::/64 eui-64
 ipv6 enable
!
router bgp 2
 bgp router-id 2.2.2.2
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2010:AB8:0:2:C600:10FF:FE58:0 remote-as 1
 !
 address-family ipv6
  neighbor 2010:AB8:0:2:C600:10FF:FE58:0 activate
 exit-address-family
!i
```

Example: Configuring BFD and Multiprotocol-BGP for IPv6

The following is a sample configuration of bidirectional forwarding detection and multiprotocol-BGP for IPv6.

Router-1

```
interface Vlan10
ipv6 address 2001:10::1/64
bfd interval 250 min_rx 250 multiplier 3
```

```
router bgp 5500
bgp router-id 9.9.9.9
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 2001:10::2 remote-as 6500
neighbor 2001:10::2 fall-over bfd
address-family ipv6
redistribute connected
neighbor 2001:10::2 activate
exit-address-family
```

Router-2

```
interface Vlan10
ipv6 address 2001:10::2/64
bfd interval 250 min_rx 250 multiplier 3
router bgp 6500
bgp router-id 10.10.10.10
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 2001:10::1 remote-as 5500
neighbor 2001:10::1 fall-over bfd
address-family ipv6
redistribute connected
neighbor 2001:10::1 activate
exit-address-family
```

Troubleshooting Tips

Problems can occur in the IPv6 functionality due to misconfigurations. To enable IPv6 functionality, you should enable IPv6 configurations at several places.

Some of the sample troubleshooting scenarios are provided below:

Problem	Solution
IPv6 commands are not available.	IPv6 is not enabled by default. Enable IPv6 functionality using **ipv6 unicast-routing** command. Also, check to see if IPv6 is enabled on the virtual templates.
No route advertisement is sent to the MN when the IPv6 CP comes up.	The route advertisement is disabled on the virtual-templates. Configure the **no ipv6 nd suppress-ra** command to enable route advertisement messages. Also, define a valid prefix pool for IPv6.

The following **debug** and **show** commands allows you to troubleshoot the IPv6 configuration.

Debug Commands	Show Commands	Platform Hardware Commands
debug ipv6	**show ipv6**	**debug platform hardware cef adjacency**
debug ipv6 address	**show ipv6 interface**	**debug platform hardware cef backwalk**
debug ipv6 icmp	**show ipv6 interface brief**	**debug platform hardware cef deaggregate**

Debug Commands	Show Commands	Platform Hardware Commands
debug ipv6 interface	**show ipv6 route**	**debug platform hardware cef entry**
debug ipv6 nd	—	**debug platform hardware cef interface**
debug ipv6 packet	—	**debug platform hardware cef loadbalance**
debug ipv6 pool	—	**debug platform hardware cef special**
debug ipv6 routing	—	**debug platform hardware cef table**
—	—	**debug platform hardware ether idb**

Where to Go Next

For additional information on IPv6 Support on the Cisco ASR 901 router, see the documentation listed in the Additional References section.

Additional References

The following sections provide references related to LLDP feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/mib/reference/asr_mib.html

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Support on the Cisco ASR 901 Router

Table 2: Feature Information for IPv6 Support on the Cisco ASR 901 Router , on page 43 lists the release history for this feature.

Table 2: Feature Information for IPv6 Support on the Cisco ASR 901 Router , on page 43 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 2: Feature Information for IPv6 Support on the Cisco ASR 901 Router , on page 43 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 2: Feature Information for IPv6 Support on the Cisco ASR 901 Router

Feature Name	Releases	Feature Information
IPv6 Support on the Cisco ASR 901 Router	15.2(2)SNG	This feature is introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:
ICMPv6	15.2(2)SNG	The ICMP is used to generate error messages. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *IPv6 Configuration Guide* provide information about this feature: • ICMP for IPv6
IPv6 Neighbor Discovery	15.2(2)SNG	The IPv6 neighbor discovery determines the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring routers. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *IPv6 Configuration Guide* provide information about this feature: • IPv6 Neighbor Discovery • IPv6 Duplicate Address Detection
IPv4 and IPv6 Dual-Stack	15.2(2)SNG	The dual IPv4 and IPv6 protocol stack technique is used to transition to IPv6. It enables gradual, one-by-one upgrades to applications running on nodes. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Dual IPv4 and IPv6 Protocol Stacks
RIP for IPv6	15.2(2)SNG	The IPv6 RIP Routing Information Database (RIB) contains a set of best-cost IPv6 RIP routes learned from all its neighboring networking devices. The RIB also stores any expired routes that the RIP process is advertising to its neighbors running RIP. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing RIP for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • RIP for IPv6

Feature Name	Releases	Feature Information
IS-IS for IPv6	15.2(2)SNG	The IPv6 RIP Routing Information Database (RIB) contains a set of best-cost IPv6 RIP routes learned from all its neighboring networking devices. The RIB also stores any expired routes that the RIP process is advertising to its neighbors running RIP. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IS-IS for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • IS-IS for IPv6
OSPFv3 for IPv6	15.2(2)SNG	OSPF is a link-state protocol. A link-state protocol makes its routing decisions based on the states of the links that connect source and destination machines. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing OSPFv3 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Information about OSPFv3
Multiprotocol BGP Extensions for IPv6	15.2(2)SNG	Multiprotocol BGP is the supported exterior gateway protocol (EGP) for IPv6. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing Multiprotocol BGP for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Multiprotocol BGP Extensions for IPv6
Bidirectional Forwarding Detection for IPv6	15.2(2)SNG	BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing Bidirectional Forwarding Detection for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Implementing Bidirectional Forwarding Detection for IPv6

Feature Name	Releases	Feature Information
Implementing QoS for IPv6	15.2(2)SNG	QoS features for IPv6 include packet classification, policing, marking on ingress path of Ethernet interfaces and packet classification, policing, marking, scheduling, per interface and per qos-group shaping, LLQ, and WRED on egress path of GigabitEthernet interfaces. **Platform-dependent Cisco IOS Software Documentation** The " Configuring QoS " section of the Cisco ASR 901 Series Aggregation Services Router Software Configuration Guide provide information about this feature: • Configuring QoS **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing QoS for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Implementing QoS for IPv6