Interface Masters
TECHNOLOGIES
Innovative Network Solutions

ISS

CLI User Manual_Vol5

INTERFACE MASTERS: ISSCLIum_Vol5/20101001

Revision Number: 28.0

Interface Masters
TECHNOLOGIES
Innovative Network Solutions

Printed in _____

DOCUMENT No.: INTERFACE MASTERS: ISSCLIum_Vol5/20101001

Contents

Chapter 41

DHCP

DHCP (Dynamic Host Configuration Protocol) allows dynamic configuration of a host computer. When a DHCP client is turned on, it initially does not have an IP address assigned to it. It sends a broadcast message to any DCHP servers that are on the network. The DHCP server assigns an IP address to the client and sends certain key network configuration parameters to the client, when an exchange takes place.

Many ISPs (Internet service providers) require that their customers use a DHCP client, so the ISP may dynamically assign IP addresses and control other network settings. Another use is for laptop computers which may be connected to more than one network. For example, a laptop may be connected to a network in the office and also at home. This is an ideal use for DHCP, as the laptop does not need to be manually reconfigured for use in the two different networks. In this case, a DHCP server is required on both office and home networks and the laptop needs a DHCP client.

The list of CLI commands for the configuration of DHCP is as follows:

DHCP Client

- debug ip dhcp client
- release
- renew
- show ip dhcp client stats

DHCP Relay

- service dhcp-relay

- ip dhcp server
- ip helper-address
- ip dhcp relay information option
- ip dhcp relay circuit-id option
- ip dhcp relay circuit id
- ip dhcp relay remote id
- debug ip dhcp relay
- show ip dhcp relay information
- show dhcp server

DHCP Server

- service dhcp-server
- service dhcp
- ip dhcp pool
- ip dhcp next-server
- ip dhcp bootfile
- bootfile config-file
- ip dhcp
- ip dhcp option
- network
- excluded-address
- ip dhcp excluded-address
- domain-name
- dns-server
- netbios-name-server
- netbios-node-type
- default-router
- option
- lease
- utilization threshold
- host hardware-type
- debug ip dhcp server
- show ip dhcp server information
- show ip dhcp server pools
- show ip dhcp server binding
- show ip dhcp server statistics

41.1 DHCP Client

DHCP client uses DHCP to temporarily receive a unique IP address for it from the DHCP server. It also receives other network configuration information such as default gateway, from the DHCP server.

41.1.1 debug ip dhcp client

This command enables the tracking of the DHCP client operations as per the configured debug levels. The debug statements are generated for the configured trace levels.

The no form of the command disables the tracking of the DHCP client operations. The debug statements are not generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

```
debug ip dhcp client { all | event | packets | errors | bind }
```

```
no debug ip dhcp client { all | event | packets | errors | bind }
```

Syntax Description

`all`	-	Generates debug statements for all kind of failure traces.
`event`	-	Generates debug statements for DHCP client events that provide DHCP client service status. The DHCP client events are generated when any of packets are sent successfully or when an ACK is received.
`packets`	-	Generates debug statements for packets related messages. These messages are generated for all events generated during processing of packets.
`errors`	-	Generates debug statements for trace error code debug messages. These messages are generated for all error events generated.
`bind`	-	Generated debug statements for trace bind messages. These messages are generated when a DHCP ACK is received.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Tracking of the DHCP client operations is disabled.

Example

```
iss# debug ip dhcp client all
```

Related Command

- **`show debugging`** – Displays state of each debugging option

41.1.2 release

This command immediately releases the DHCP lease obtained for an IP address from a DHCP server and assigned to the specified interface. The current lease assigned to that interface is terminated manually.

The lease is terminated to reset the DHCP client which faces connectivity problem. The DHCP lease provided by the DHCP server represents the time interval till which the DHCP client can use the assigned IP address.

```
release dhcp { vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }
```

Syntax Description

vlan - Releases the DHCP lease for the specified VLAN ID. This is a unique value that represents the specific VLAN created.

This value ranges between 1 and 4094.

<interface-type> - Releases the DHCP lease for the specified type of interface. The interface can be:

- fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
- gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
- extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- i-lan – Internal LAN created on a bridge per IEEE 802.1ap.

<interface-id> - Releases the DHCP lease for the specified interface identifier. This is a unique value that represents the specific interface.

This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. For example: 0/1 represents that the slot number is 0 and port number is 1.

Only i-lan ID is provided for interface type i-lan. For example: 1 represents i-lan ID.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# release dhcp vlan 1
```

☞ This command executes successfully only if the VLAN interfaces and router ports are in BOUND state (that is, IP address is dynamically acquired from DHCP server and an active lease is bound to the interface). The port should have been configured as router port for dynamically acquiring an IP address from DHCP server.

Related Commands

- **`no switchport`** – Configures the port as a router port.
- **`ip address – rarp/dhcp`** - Configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server.
- **`show ip dhcp client stats –`** Displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server.
- **`show ip interfaces –`** Displays the IP interface configuration for all interfaces available in the switch.

41.1.3 renew

This command immediately renews the DHCP lease for the interface specified. The current lease acquired by the specified interface is manually renewed or else a new DHCP lease is acquired for interface whose lease is terminated. The DHCP lease is automatically renewed, once the lease expires.

```
renew dhcp { vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }
```

Syntax Description

vlan	- Renews the DHCP lease for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
<interface-type>	- Renews the DHCP lease for the specified type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan – Internal LAN created on a bridge per IEEE 802.1ap.
<interface-id>	- Renews the DHCP lease for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided for interface type i-lan. For example: 1 represents i-lan ID.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# renew dhcp vlan 1
```

☞ This command executes successfully only if the VLAN interfaces and router ports are in BOUND state (that is, IP address is dynamically acquired from DHCP server

and an active lease is bound to the interface). The port should have been configured as router port for dynamically acquiring an IP address from DHCP server.

Related Commands

- **`no switchport`** – Configures the port as a router port.
- **`ip address – rarp/dhcp`** - Configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server.
- **`show ip dhcp client stats –`** Displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server.
- **`show ip interface –`** Displays the IP interface configuration for all interfaces available in the switch.

41.1.4 show ip dhcp client stats

This command displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server.

The statistics information contains interface name, IP address assigned by DHCP server, DHCP lease details, details regarding number of DHCPDISCOVER, DHCPREQUEST, DHCPDECLINE, DHCPRELEASE and DHCPINFORM packets received and number of DHCPOFFER packets sent from the DHCP client.

show ip dhcp client stats

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ip dhcp client stats

Dhcp Client Statistics
--------------------------

Interface                    : vlan1
Client IP Address            : 12.0.0.21
Client Lease Time            : 3600
Client Remain Lease Time     : 3569
Message Statistics
------------------
DHCP DISCOVER                : 1
DHCP REQUEST                 : 1
DHCP DECLINE                 : 0
DHCP RELEASE                 : 0
DHCP INFORM                  : 0
DHCP OFFER                   : 1
```

Related Commands

- **ip address – rarp/dhcp –** Configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server.
- **release** - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- **renew –** Renews the DHCP lease for the interface specified.

41.2 DHCP Relay

DHCP relay agent is a host or an IP router that allows the DHCP client and DHCP server in different subnets to communicate with each other, so that the DHCP client can obtain its configuration information while booting. The relay agent receives packets from the client, inserts information such as network details, and forwards the modified packets to the server. The server identifies the client's network from the received packets, allocates the IP address accordingly, and sends reply to the relay. The relay strips the information inserted by the server and broadcasts the packets to the client's network.

41.2.1 service dhcp-relay

This command enables the DHCP relay agent in the switch.

The no form of the command disables the DHCP relay agent.

DHCP relay agent relays DHCP messages between DHCP client and DHCP server located in different subnets.

`service dhcp-relay`

`no service dhcp-relay`

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults DHCP relay agent is disabled (that is, the switch acts as a DHCP client)

Example

```
iss(config)# service dhcp-relay
```

☞ The DHCP relay agent can be enabled in the switch, only if the DHCP server is disabled in the switch.

Related Commands

- **`no service dhcp-service`** – Disables the DHCP server.
- **`show ip dhcp relay information`** - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

41.2.2 ip dhcp server

This command adds the configured IP address to the IP address list created for the DHCP server. The switches or systems having these IP addresses represent the DHCP servers to which the DHCP relay agent can forward the packets that are received from DHCP clients.

The no form of the command deletes the mentioned IP address from the IP address list..

The DHCP relay agent broadcasts the received packets to entire network except the network from which the packets are received, if the DHCP server list is empty (that is IP address is configured as 0.0.0.0).

The IP address can be added or deleted from the IP address list, even if the DHCP relay agent is disabled; but the packets are not forwarded. The packets are forwarded, only if the DHCP relay agent is enabled.

- The IP address list can contain only 5 IP addresses (that is, only a maximum of 5 DHCP servers can be listed).

ip dhcp server <ip address>

no ip dhcp server <ip address>

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	0.0.0.0 (that is, DHCP server list is empty)
Example	`iss(config)# ip dhcp server 12.0.0.1`
Related Commands	• **show ip dhcp relay information** - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured. • **show dhcp server –** Displays the DHCP servers' IP addresses

41.2.3 ip helper-address

This command sets the IP address of the DHCP Server. The Relay Agent now starts forwarding the packets (that is, UDP broadcasts including BOOTP) from the client to the specified DHCP Server. This command allows to add more than one DHCP Server.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip dhcp server. This command also explicitly enables the DHCP relay and disables the DHCP Server.

`ip helper-address <ip address>`

Syntax Description	**`ip address`**	-	IP address of the server to which the packets are to be forwarded

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults The IP address is 0.0.0.0 and the status of the **DHCP Relay Servers only** is disabled.

Example

```
iss(config-if)# ip helper-address 12.0.0.1
```

☞

- The Relay Agent will start forwarding the packets from the client to a specific DHCP Server only when the Relay Agent is in the enabled state.

Related Commands

- **`show ip dhcp relay information`** - Displays the DHCP relay information
- **`show dhcp server – Displays the DHCP Server information`**

41.2.4 ip dhcp relay information option

This command enables the DHCP relay agent to perform processing related to DHCP relay agent information option.

The no form of the command disables the processing related to DHCP relay agent information option.

The options contains a sub-option for agent circuit ID details and another sub-option for agent remote ID details. The processing involves:

- Insertion of DHCP relay information option in DHCP request messages forwarded to a DHCP server from a DHCP client.
- Examining / removing of DHCP relay information option from DHCP response messages forwarded to the DHCP client from the DHCP server.

The processing of DHCP relay agent information option can be enabled or disabled, even if the DHCP relay agent is disabled; but no messages are forwarded and processed. The messages are forwarded and processed, only if the DHCP relay agent is enabled.

`ip dhcp relay information option`

`no ip dhcp relay information option`

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Processing related to DHCP relay agent information option is disabled.

Example

```
iss(config)# ip dhcp relay information option
```

Related Commands

- **`ip dhcp relay circuit-id option`** – Defines the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option.
- **`show ip dhcp relay information`** - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

41.2.5 ip dhcp relay circuit-id option

This command defines the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option.

ip dhcp relay circuit-id option [router-index] [vlanid] [recv-port]

Syntax Description

router-index	-	Adds information related to router interface indexes in the circuit ID sub-option.
vlanid	-	Adds information related to VLAN IDs in the circuit ID sub-option.
recv-port	-	Adds information related to physical interfaces or LAG ports in the circuit ID sub-option

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults router-index

Example

```
iss(config)# ip dhcp relay circuit-id option vlanid
```

☞ The type of information to be present in the circuit ID sub-option can be configured, only if the DHCP relay agent is enabled to perform processing related to DHCP relay agent information option.

Related Commands

- **ip dhcp relay information option –** Enables the DHCP relay agent to perform processing related to DHCP relay agent information option.
- **show ip dhcp relay information** - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

41.2.6 ip dhcp relay circuit id

This command configures circuit ID value for an interface.

The no form of the command deletes the circuit ID configuration for the interface (that is, the circuit ID is configured as 0).

The circuit ID uniquely identifies a circuit over which the incoming DHCP packet is received. In DHCP relay, it is used to identify the correct circuit over which the DHCP responses should be relayed.

The configured circuit ID is used in the DHCP relay agent information option to inform the DHCP server about the interface from which DHCP packet is received. The circuit ID is unique for the interfaces and ranges from 1 to 2147483647.

The minimum value depends upon the number of interfaces that can be created. For example, if a total of 160 interfaces are allowed to be created in the switch, then the circuit ID value range starts from 161 only. The interfaces include all physical interfaces, port channels and logical L3 interfaces.

ip dhcp relay circuit-id <circuit-id>

no ip dhcp relay circuit-id

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config-if)# ip dhcp relay circuit-id 1
```

☞ This command is available only for the VLAN interfaces and ports that are configured as router ports.

Related Commands

- **no switchport** – Configures the port as a router port.
- **show ip dhcp relay information** - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

41.2.7 ip dhcp relay remote id

This command configures remote ID value for an interface.

The no form of the command deletes the remote ID configuration for the interface (that is, the remote ID is set with a string of length zero).

The configured remote ID is used in the DHCP relay agent information option to inform the DHCP client about the remote circuit to which the DHCP packets should be forwarded from the interface. The remote ID is globally unique and an octet string of maximum size of 32. The remote ID should not be same as that of the default value.

ip dhcp relay remote-id <remote-id name>

no ip dhcp relay remote-id

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults XYZ. This value is internally assigned.

Example

```
iss(config-if)# ip dhcp relay remote-id Interface Masters
```

☞ This command is available only for the VLAN interfaces and ports that are configured as router ports.

Related Commands

- **no switchport** – Configures the port as a router port.
- **show ip dhcp relay information** - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

41.2.8 debug ip dhcp relay

This command enables the tracking of the DHCP relay module operations as per the configured debug levels. The debug statements are generated for the configured trace level.

The no form of the command disables the tracking of the DHCP relay module operations. The debug statements are not generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

debug ip dhcp relay {all | errors}

no debug ip dhcp relay {all | errors}

Syntax Description	**all**	-	Generates debug statements for all kind of failure traces.
	errors	-	Generates debug statements for trace error code debug messages. These messages are generated for all error events generated.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Tracking of the DHCP relay module operation is disabled.

Example
```
iss# debug ip dhcp relay all
```

Related Commands **show ip dhcp relay information** -Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

41.2.9 show ip dhcp relay information

This command displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

The information contains status of the DHCP relay, DHCP server IP addresses, status of relay information option, configured debug level and statistics details regarding number of packets affected by relay information option, circuit ID suboption, remote ID suboption, and subnet mask sub option.

show ip dhcp relay information [vlan <vlan-id>]

Syntax Description

vlan	-	Displays the DHCP relay agent configuration information for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ip dhcp relay information

Dhcp Relay                    : Enabled
Dhcp Relay Servers only       : Enabled

DHCP server 1                 : 12.0.0.1

Dhcp Relay RAI option         : Enabled
Default Circuit Id information : router-index
Debug Level                   : 0x1

No of Packets inserted RAI option               : 0
No of Packets inserted circuit ID suboption     : 0
No of Packets inserted remote ID suboption      : 0
No of Packets inserted subnet mask suboption    : 0
No of Packets dropped                           : 0
No of Packets which did not inserted RAI option : 0


 Interface  vlan1
Circuit ID : 162
Remote  ID : 45
```

Related Commands

- **service dhcp-relay** - Enables the DHCP relay agent in the switch.
- **ip dhcp server** - Adds the configured IP address to the IP address list created for the DHCP server.
- **ip dhcp relay information option –** Enables the DHCP relay agent to perform processing related to DHCP relay agent information option.
- **ip dhcp relay circuit-id option –** Defines the type of information to

be present in circuit ID sub-option that is used in the DHCP relay agent information option.

- **`ip dhcp relay circuit-id`** – Configures circuit ID value for an interface.
- **`ip dhcp relay remote-id`** – Configures remote ID value for an interface.
- **`debug ip dhcp relay`** – Enables the tracking of the DHCP relay module operations as per the configured debug levels

41.2.10 show dhcp server

This command displays the DHCP servers' IP addresses. These addresses denotes the PCs or switches that can act as a DHCP server.

show dhcp server

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show dhcp server

DHCP server:  40.0.0.4
```

Related Commands

- **ip dhcp server –** Adds the configured IP address to the IP address list created for the DHCP server.

41.3 DHCP Server

DHCP server is responsible for dynamically assigning unique IP address and other configuration parameters such as gateway, to interfaces of a DHCP client. The IP address is leased to the interface only for a particular time period as mentioned in the DHCP lease. The interface should renew the DHCP lease once it expires. The DHCP server contains a pool of IP address from which one address is assigned to the interface.

41.3.1 service dhcp-server

This command enables the DHCP server in the switch (that is, switch acts as DHCP server).

The no form of the command disables the DHCP server in the switch.

The DHCP server assigns unique IP address and other configuration parameters such as gateway, to interfaces of a DHCP client.

service dhcp-server

no service dhcp-server

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults DHCP server is disabled (that is, the switch acts as a DHCP client)

Example

```
iss (config)# service dhcp-server
```

☞ The DHCP server can be enabled in the switch, only if the DHCP relay agent is disabled in the switch.

Related Commands

- **no service dhcp-relay –** Disables the DHCP relay agent in the switch.
- **show ip dhcp server information** - Displays the DHCP server configuration information.
- **show ip dhcp server binding** - Displays the DHCP server binding information
- **show ip dhcp server statistics** - Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

41.3.2 service dhcp

This command enables the DHCP Server. The no form of this command disables the DHCP Server.

This command is a complete standardized implementation of the existing command and operates similar to that of the command service dhcp-server.

`service dhcp`

`no service dhcp`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	DHCP Server is disabled.
Example	`iss(config)# service dhcp`
☞	DHCP Relay must be disabled before enabling the DHCP Server.
Related Command	• **`no service dhcp-relay`** – Disables the DHCP Relay • **`show ip dhcp server information`** - Displays the DHCP Server information

41.3.3 ip dhcp pool

This command creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.

The no form of the command deletes the existing DHCP server address pool.

The address pool has a range of IP addresses that can be assigned to the DHCP client and also information about client configuration parameters such as domain name. The pool created is identified with a unique ID whose value ranges from 1 to 2147483647.

ip dhcp pool <index (1-2147483647)>

no ip dhcp pool <index (1-2147483647)>

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example
```
iss (config)# ip dhcp pool 1
```

Related Commands

- **network** - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **excluded-address** - Creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool.
- **domain-name –** Configures the domain name option for the corresponding DHCP server address pool.
- **dns-server** - Configures the IP address of a DNS server for the corresponding DHCP server address pool.
- **netbios-name-server** - Configures the IP address of a NetBIOS and WINS name server that is available to Microsoft DHCP clients.
- **netbios-node-type –** Configures the NetBIOS node type for Microsoft DHCP clients, for the corresponding DHCP server address pool.
- **default-router** - Configures the IP address of a default router to which a DHCP client should send packets after booting, for the corresponding DHCP server address pool.
- **option** - Configures, for the corresponding DHCP server address pool, the various available DHCP server options with the corresponding specific values.
- **lease** - Configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.
- **utilization threshold** - Configures pool utilization threshold value (in percentage) for the corresponding DHCP server address pool.
- **host hardware-type** - Configures host hardware type and its DHCP option

with specific values for the corresponding DHCP server address pool.

- **`show ip dhcp server pools`** - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.
- **`show ip dhcp server statistics`** - Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

41.3.4 ip dhcp next-server

This command sets the IP address of the boot server (that is, TFTP server) from which the initial boot file is to be loaded in a DHCP client. This boot server acts as a secondary server.

The no form of the command deletes the boot server details and resets to its default value.

The DHCP server is used as the boot server, if no TFTP server is configured as the boot server.

ip dhcp next-server <ip address>

no ip dhcp next-server

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	0.0.0.0 (No boot server is defined. DHCP server is used as the boot server)
Example	`iss (config)# ip dhcp next-server 12.0.0.1`
Related Commands	• **ip dhcp bootfile** - Configures the name of the initial boot file to be loaded in a DHCP client. • **show ip dhcp server information** - Displays the DHCP server configuration information

41.3.5 ip dhcp bootfile

This command configures the name of the initial boot file to be loaded in a DHCP client. The file name is a string whose maximum size is 63.

The no form of the command deletes the boot file name (that is, no file is specified as the initial boot file).

The boot file contains the boot image that is used as the operating system for the DHCP client.

ip dhcp bootfile <bootfile (63)>

no ip dhcp bootfile

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss (config)# ip dhcp bootfile 53
```

Related Commands

- **ip dhcp next-server** - Sets the IP address of the boot server (that is, TFTP server) from which the initial boot file is to be loaded.
- **show ip dhcp server information** - Displays the DHCP server configuration information

41.3.6 bootfile config-file

This command defines the name of the boot image file that the DHCP client should download during auto install process. The DHCP Server passes this file name to the DHCP client. The no form of this command deletes the specified boot file name and assigns the value of boot file name as None (that is, no file is set as boot image file).

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip dhcp bootfile.

bootfile config-file <bootfile (63)>

no bootfile config-file

Syntax Description	**bootfile**	- Name of the boot image file that should be downloaded by the DHCP client.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	None (Null terminated string)	
Example	`iss(config)# bootfile config-file boot.img`	
Related Commands	• **show ip dhcp server information** - Displays the DHCP Server information	

41.3.7 ip dhcp

This command enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server. These parameters are used to control the allocation of IP address to a DHCP client.

The no form of the command disables ICMP echo mechanism, resets server offer-reuse time to its default value or removes a bind entry from a server binding table.

```
ip dhcp { ping packets [<count(0-10)>] | server offer-reuse <timeout (1-120)>
}
```

```
no ip dhcp { ping packets | server offer-reuse | binding <ip address> }
```

Syntax Description

`ping packets [<count(0-10)>]`	-	Enables / disables ICMP echo mechanism. This mechanism allows the DHCP server to verify the availability of an IP address before assigning it to a DHCP client. DHCP server sends ping packets to the IP address that is intended to be assigned for the DHCP client. If the ping operation fails, DHCP server assumes that the address is not in use and assigns the address to the requesting DHCP client. <count(0-10)> - Configures the number of ping packets to be sent from the DHCP server to the pool address before assigning the address to a requesting client. The pinging of pool addresses is disabled, if the count value is set as 0. This value ranges from 0 to 10. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
`server offer-reuse`	-	Configures the amount of time (in seconds), the DHCP server entity should wait for the DHCP REQUEST from the DHCP client before reusing the lease offer for other DHCP client. This value ranges between 1 and 120 seconds.
`binding`	-	Deletes the specified IP address entry from the server binding table. This frees the IP address allocated to a DHCP client, so that the IP address can be allocated for another DHCP client.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults

ping packets	-	ICMP echo mechanism feature is disabled.

server offer-reuse - 5

Example

```
iss (config)# ip dhcp ping packets
```

Related Commands

- **`show ip dhcp server information`** - Displays the DHCP server configuration information.
- **`show ip dhcp server binding`** – Displays the DHCP server binding information.
- **`show ip dhcp server statistics`** - Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

41.3.8 ip dhcp option

This command sets the DHCP Server options.

This command globally configures the various available DHCP server options with the corresponding specific values. These values can be an ASCII string, hexadecimal string or IP address. These global options are applicable for all DHCP server address pools.

The no form of the command deletes the existing DHCP server option.

```
ip dhcp option <code (1-2147483647)> { ascii <string> | hex <Hex String> | ip
<address> }
```

```
no ip dhcp option <code (1-2147483647)>
```

Syntax Description

`<code (1-2147483647)>`	-	Specifies the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message. This value ranges from 1 to 2147483647.
`ascii`	-	Specifies the ASCII value to be set for the corresponding option code that accepts ASCII string. This value is a character string that should contain only characters from NVT ASCII character set.
`hex`	-	Specifies the hexadecimal value to be set for the corresponding option code that accepts hexadecimal string.
`ip`	-	Specifies the unicast IP address to be set for the corresponding option code that accepts IP address.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config)# ip dhcp option 19 hex d
```

Related Commands

- **`show ip dhcp server pools`** - Displays global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.9 network

This command creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.

The no form of the command deletes the created subnet pool.

```
network <network- IP> [ { <mask> | / <prefix-length (1-31)> } ] [end ip]
```

```
no network
```

Syntax Description

`<network-IP>`	-	Configures the network IP subnet address for the DHCP pool. The addresses within the specified network subnet are assigned to the DHCP client, if no restriction is applied. For example: The value is configured as 20.0.0.0, then any one of the address within the range from 20.0.0.1 to 20.255.255.255 can be assigned to the DHCP client if no other limitations such as end IP address, are set. This value should be unique (that is, one subnet address can be assigned only for one DHCP address pool).
`<mask>`	-	Configures the subnet mask for the network IP address. This is a 32-bit number which is used to divide the IP address into network address and host address. This value is used to automatically calculate the end IP address for the pool. For example: The value 254.0.0.0 represents that the end IP address is 21.255.255.255, if the network subnet is set as 20.0.0.0.
`/ <prefix-length (1-31)>`	-	Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value should be preceded by a slash (/) with space before and after the slash. This value is used to automatically calculate the end IP address for the pool and set the mask for the subnet. For example: value 20.0.0.0 / 6 represents that the end ip address is 23.255.255.255 and the mask is 252.0.0.0.
`<end ip>`	-	Configures the end IP address for the network IP subnet set for the DHCP address pool. This value restricts the IP addresses that can be assigned to the DHCP client. This value is used to manually set the end IP address. This value overrides the end IP address calculated

automatically using the mask or prefix-length.

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults

<mask>	-	255.0.0.0
<end ip>	-	Represents the last possible subnet address. For example: If network subnet address is mentioned as 20.0.0.0, then end IP address would be 20.255.255.255.

Example

```
iss(dhcp-config)# network 20.0.0.0 255.0.0.0 20.0.0.50
```

Related Commands

- **`ip dhcp pool`** – Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **`excluded-address`** – Creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool.
- **`domain-name`** – Configures the domain name option for the corresponding DHCP server address pool.
- **`dns-server`** – Configures the IP address of a DNS server for the corresponding DHCP server address pool.
- **`netbios-name-server`** – Configures the IP address of a NetBIOS and WINS name server that is available to Microsoft DHCP clients.
- **`netbios-node-type`** - Configures the NetBIOS node type for Microsoft DHCP clients, for the corresponding DHCP server address pool.
- **`netbios-node-type`** – Configures the IP address of a default router to which a DHCP client should send packets after booting, for the corresponding DHCP server address pool.
- **`option`** – Configures, for the corresponding DHCP server address pool, the various available DHCP server options with the corresponding specific values.
- **`Lease`** – Configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.
- **`utilization threshold`** – Configures pool utilization threshold value (in percentage) for the corresponding DHCP server address pool.
- **`show ip dhcp server pools`** – Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.10 excluded-address

This command creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool. That is, the IP addresses in this range including start and end IP address of the excluded pool are not assigned to any DHCP client..

The no form of the command deletes the created excluded pool. The same start IP address and end IP address of the already created excluded pool should be provided while executing the no form of the command.

excluded-address <low-address> <high-address>

no excluded-address <low-address> [<high-address>]

Syntax Description

<low-address> - Sets the start IP address for an excluded pool. This address denotes the first IP address of a range of IP addresses which needs to be excluded from the created subnet pool.

This IP address should be:

- low than the end IP address, and
- in the same network of the subnet pool's start IP address.

<high-address> - Sets the end IP address for an excluded pool. This address denotes the last IP address of a range of IP addresses which needs to be excluded from the created subnet pool.

This IP address should be:

- high than the start IP address, and
- within or equal to the subnet pool's end IP address.

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(dhcp-config)# excluded-address 20.0.0.1 20.0.0.30
```

☞ This command is executed successfully, only if a subnet pool is already created for the DHCP address pool.

Related Commands

- **ip dhcp pool** – Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **network** – Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **show ip dhcp server pools** – Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.11 ip dhcp excluded-address

This command creates an excluded pool to prevent DHCP Server from assigning certain addresses to DHCP clients. The no form of the command deletes the excluded pool.

This command is a complete standardized implementation of the existing command and operates similar to that of the command excluded-address. This command is used to exclude a single IP address or a range of IP addresses.

```
ip dhcp excluded-address <low-address> [<high-address>]
```

```
no ip dhcp excluded-address <low-address> [high-address]
```

Syntax Description

low-address	-	The excluded IP address, or first IP address in an excluded address range
high-address	-	The last IP address in the excluded address range

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config)# ip dhcp excluded-address 20.0.0.20 20.0.0.30
```

- The DHCP Server assumes that all pool addresses may be assigned to clients.

Subnet pool should have been created before creating an excluded pool. This excluded pool should be within the range of the created subnet pool. For example, the excluded pool 20.0.0.20 – 20.0.0.30 created using this command is within the already created subnet pool 20.0.0.0 – 20.0.0.100.

Related Commands

- **ip dhcp pool –** Creates a DHCP Server address pool and places the user in the DHCP pool configuration mode
- **network –** Sets the network IP and mask in DHCP Server configuration parameters
- **service dhcp-server –** Enables the DHCP Server
- **show ip dhcp server information –** Displays the server information
- **show ip dhcp server pools –** Displays the DHCP Server pools
- **show ip dhcp server binding –** Displays the DHCP Server binding information
- **show ip dhcp server statistics –** Displays the DHCP Server statistics

41.3.12 domain-name

This command configures the domain name option for the corresponding DHCP server address pool. A DHCP client uses this domain name while resolving host names through a domain name system. The DHCP option code is 15. This value is a string whose maximum size is 63.

The no form of the command deletes the domain name option configuration for the DHCP server address pool. The domain name option configuration is deleted, if the no form of the network command is executed successfully.

domain-name <domain (63)>

no domain-name

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(dhcp-config)# domain-name Interface Masters
```

☞ The domain name configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Related Commands

- **ip dhcp pool** – Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **network** – Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **show ip dhcp server pools** – Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.13 dns-server

This command configures the IP address of a DNS server for the corresponding DHCP server address pool. The client correlates the DNS IP address with the host name. The DNS server is used to translate domain names and hostnames into corresponding IP addresses.

The no form of the command deletes the DNS server IP address option configuration for the DHCP server address pool. The DNS server IP address option configuration is deleted, if the no form of the network command is executed successfully.

dns-server <ip address>

no dns-server

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Example
```
iss(dhcp-config)# dns-server 20.0.0.1
```

☞ The DNS server IP address configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Related Commands

- **ip dhcp pool –** Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **network –** Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **show ip dhcp server pools –** Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.14 netbios-name-server

This command configures, for the corresponding DHCP server address pool, the IP address of a NetBIOS (Network Basic Input / Output System) and WINS (Windows Internet Naming Service) name server that is available to Microsoft DHCP clients.

The no form of the command deletes the NetBIOS and WINS name server IP address configuration for the DHCP server address pool. The NetBIOS WINS name server option configuration is deleted, if the no form of the network command is executed successfully.

The NetBIOS name server provides the following three distinct services:

1. Name service for name registration and resolution
2. Session service for connection oriented communication
3. Datagram distribution service for connectionless communication

`netbios-name-server <ip address>`

`no netbios-name-server`

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(dhcp-config)# netbios-name-server 20.0.0.3
```

☞ The NetBIOS WINS name server configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Related Commands

- **`ip dhcp pool`** – Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **`network`** – Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **`show ip dhco server pools`** – Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.15 netbios-node-type

This command configures the NetBIOS node type for Microsoft DHCP clients, for the corresponding DHCP server address pool.

The no form of the command deletes the NetBIOS node type option configuration for the DHCP server address pool. The NetBIOS node type option configuration is deleted, if the no form of the network command is executed successfully.

The node type denotes the method used to register and resolve NetBIOS names to IP addresses.

```
netbios-node-type { <0-FF> | b-node | h-node | m-node | p-node }
```

```
no netbios-node-type
```

Syntax Description

`<0-FF>`	-	Allows NetBIOS over TCP/IP clients. This value ranges from 0 to 255.
`b-node`	-	Configures the DHCP server address pool to broadcast IP messages for registering and resolving NetBIOS names to IP addresses. The node type value is set as 1.
`h-node`	-	Configures the DHCP server address pool to initially query name server and subsequently broadcast IP messages for registering and resolving NetBIOS names to IP addresses. The node type value is set as 8. This node type is the best option for all conditions.
`m-node`	-	Configures the DHCP server address pool to initially broadcast IP message and then query name server for registering and resolving NetBIOS names to IP addresses. The node type value is set as 4.
`p-node`	-	Configures the DHCP server address pool to have point-to-point communication with a NetBIOS name server for registering and resolving NetBIOS names to IP addresses. The node type value is set as 2.

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(dhcp-config)# netbios-node-type h-node
```

☞ The NetBIOS node type configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Related Commands

- **`ip dhcp pool`** – Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **`network`** – Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **`show ip dhcp server pools`** – Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.16 default-router

This command configures the IP address of a default router to which a DHCP client should send packets after booting, for the corresponding DHCP server address pool.

The no form of the command deletes the default router IP address configuration for the DHCP server address pool. The default router IP address configuration is deleted, if the no form of the network command is executed successfully.

default-router <ip address>

no default-router

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(dhcp-config)# default-router 10.23.2.99
```

- The configured IP address of the default router should be on the same subnet of the DHCP client.
- The default router IP address configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Related Commands

- **ip dhcp pool –** Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **network** - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **show ip dhcp server pools –** Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.17 option

This command configures, for the corresponding DHCP server address pool, the various available DHCP server options with the corresponding specific values. These values can be an ASCII string, hexadecimal string or IP address.

The no form of the command deletes the DHCP server option for the DHCP server address pool. The DHCP server option configuration is deleted, if the no form of the network command is executed successfully.

```
option <code (1-2147483647)> { ascii <string> | hex <Hex String> | ip <address> }

no option <code (1-2147483647)>
```

Syntax Description

<code (1-2147483647)	-	Specifies the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message on response to a DHCP DISCOVER message. This value ranges from 1 to 2147483647.
ascii	-	Specifies the ASCII value to be set for the corresponding option code that accepts ASCII string. This value is a character string that should contain only characters from NVT ASCII character set.
hex	-	Specifies the hexadecimal value to be set for the corresponding option code that accepts hexadecimal string.
ip	-	Specifies the unicast IP address to be set for the corresponding option code that accepts IP address.

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults

<code (1-2147483647)	-	1
ip	-	255.0.0.0

Example

```
iss(dhcp-config) # option 19 hex f
```

☞ The DHCP server options configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Related Commands

- **ip dhcp pool –** Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.

- **`network –`** Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **`show ip dhcp server pools –`** Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.18 lease

This command configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.

The no form of the command resets the DHCP lease period to its default value for the DHCP server address pool. The DHCP lease period configuration is deleted and reset, if the no form of the network command is executed successfully.

The DHCP lease period represents the time interval (in seconds) till which the DHCP client can use the assigned IP address. The time interval is internally calculated in seconds based on the number of days, hours and minutes configuration.

```
lease { <days (0-365)> [<hours (0-23)> [<minutes (1-59)>]] | infinite }
```

```
no lease
```

Syntax Description

`<days (0-365)>`	-	Configures the number of days that is used to calculate the DHCP lease period. The period also depends on the configured number of hours and minutes. This value ranges from 0 to 365. The value 0 is valid only if either number of hours or minutes is configured with any value other than 0.
`<hours (0-23)>`	-	Configures the number of hours that is used to calculate the DHCP lease period. The period also depends on the configured number of days and minutes. This value ranges from 0 to 23. The value 0 is valid only if either number of days or minutes is configured with any value other than 0.
`<minutes (1-59)>`	-	Configures the number of minutes that is used to calculate the DHCP lease period. The period also depends on the configured number of days and hours. This value ranges from 1 to 59.
`infinite`	-	Configures the DHCP lease period as 2147483647 seconds.

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 3600 seconds (that is, 1 hour)

Example

```
iss(dhcp-config)# lease 1
```

☞ The DHCP lease period configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Related Commands

- **`ip dhcp pool`** – Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **`network`** – Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **`show ip dhcp server pools`** - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.19 utilization threshold

This command configures pool utilization threshold value (in percentage) for the corresponding DHCP server address pool.

The no form of the command resets the pool utilization threshold to its default value for the DHCP server address pool.

If the pool utilization exceeds the configured threshold value, a syslog event and an SNMP trap message are generated. The threshold value ranges from 0 to 100 percentage.

```
utilization threshold { <integer (0-100)> }
```

```
no utilization threshold
```

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 75 percent

Example

```
iss(dhcp-config)# utilization threshold 76
```

☞ The pool utilization threshold configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Related Commands

- **`ip dhcp pool`** – Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **`network`** – Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- **`show ip dhcp server pools`** - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

41.3.20 host hardware-type

This command configures host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool.

The no form of the command deletes the hardware type and its DHCP option.

```
host hardware-type <type (1-2147483647)> client-identifier <mac-address> { ip
<address> | option <code (1-2147483647)> { ascii <string> | hex <Hex String> |
ip <address> }}
```

```
no host hardware-type <host-hardware-type (1-2147483647)> client-identifier
<client-mac-address> [{ ip | option <code (1-2147483647)> }]
```

Syntax Description

`<type (1-2147483647)>`	-	Specifies the host hardware type for which the host address and the DHCP options needs to be configured. This value ranges from 1 to 2147483647. Only the value 1 is supported, which represents that the hardware type is Ethernet.
`client identifier`	-	Specifies the DHCP client identifier in a host declaration so that a host record can be found using this client identifier. The client identifier represents the physical address (MAC address) of a network card.
`ip`	-	Configures the IPv4 address for the DHCP host.
`option`	-	Specifies the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message on response to a DHCP DISCOVER message. This value ranges from 1 to 2147483647. • ascii - Specifies the ASCII value to be set for the corresponding option code that accepts ASCII string. This value is a character string that should contain only characters from NVT ASCII character set. • hex - Specifies the hexadecimal value to be set for the corresponding option code that accepts hexadecimal string. • ip - Specifies the unicast IP address to be set for the corresponding option code that accepts IP address.

Mode DHCP Pool Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(dhcp-config)# host hardware-type 1 client-identifier
00:11:22:33:44:55 option 1 ip 10.0.0.1
```

Related Commands

- **`ip dhcp pool`** – Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **`show ip dhcp server pools`** - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.
- **`show ip dhcp server binding`** – Displays the DHCP server binding information

41.3.21 debug ip dhcp server

This command enables the tracking of the DHCP server operations as per the configured debug levels. The debug statements are generated for the configured trace levels.

The no form of the command disables the tracking of the DHCP server operations. The debug statements are not generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

```
debug ip dhcp server { all | events | packets | errors | bind | linkage }
```

```
no debug ip dhcp server { all | events | packets | errors | bind | linkage}
```

Syntax Description

`all`	-	Generates debug statements for all kind of failure traces.
`events`	-	Generates debug statements for DHCP server events that provide DHCP server service status. The DHCP server events are generated when any of packets are sent successfully or when an ACK is received.
`packets`	-	Generates debug statements for packet related messages. These messages are generated for all events generated during processing of packets.
`errors`	-	Generates debug statements for trace error code debug messages. These messages are generated for all error events generated.
`bind`	-	Generates debug statements for trace bind messages. These messages are generated when a DHCP ACK is received.
`linkage`	-	Generates debug statements for database linkage messages. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Tracking of the DHCP server operations is disabled

Example

```
iss# debug ip dhcp server all
```

Related Commands

- **`show ip dhcp server information`** – Displays the DHCP server configuration information.
- **`show debugging`** - Displays state of each debugging option

41.3.22 show ip dhcp server information

This command displays the DHCP server configuration information.

The information contains status of DHCP server, ICMP echo mechanism status, debug level, boot server IP address, boot file name and server offer reuse time.

show ip dhcp server information

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ip dhcp server information

DHCP server status                  : Enable
Send Ping Packets                   : Disable
Debug level                         : None
Server Address Reuse Timeout        : 5 secs
Next Server Adress                  : 0.0.0.0
Boot file name                      : None
```

Related Commands

- **service dhcp-server –** Enables the DHCP server in the switch (that is, switch acts as DHCP server).
- **ip dhcp next-server –** Sets the IP address of the boot server (that is, TFTP server) from which the initial boot file is to be loaded.
- **ip dhcp bootfile –** Configures the name of the initial boot file to be loaded in a DHCP client.
- **ip dhcp –** Enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server.
- **debug ip dhcp server** - Enables the tracking of the DHCP server operations as per the configured debug levels.

41.3.23 show ip dhcp server pools

This command displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

show ip dhcp server pools

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ip dhcp server pools
 Global Options
--------------

Code       :    19, Value      : 0

Pool Id                         : 1
-----------------------------------------
Subnet                          : 20.0.0.0
Subnet Mask                     : 255.0.0.0
Lease time                      : 86400 secs
Utilization threshold           : 76%
Start Ip                        : 20.0.0.1
End Ip                          : 20.0.0.50
Exclude Address Start IP        : 20.0.0.1
Exclude Address End IP          : 20.0.0.30

Subnet Options
--------------
Code       :     1, Value      : 255.0.0.0
Code       :     3, Value      : 10.23.2.99
Code       :     6, Value      : 20.0.0.1
Code       :    15, Value      : Interface Masters
Code       :    19, Value      : 0
Code       :    44, Value      : 20.0.0.3
Code       :    46, Value      : 8

Host Options
------------
Hardware type                   : 1
Client Identifier               : 00:11:22:33:44:55
Code       :     1, Value      : 10.0.0.1
```

Related Commands

- **ip dhcp option** - Configures globally the various available DHCP server options with the corresponding specific values
- **ip dhcp pool** - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **network –** Creates a subnet pool that defines a network IP subnet address for

the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.

- **Excluded-address –** Creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool.
- **domain-name –** Configures the domain name option for the corresponding DHCP server address pool.
- **dns-server** - Configures the IP address of a DNS server for the corresponding DHCP server address pool.
- **netbios-name-server** - Configures the IP address of a NetBIOS and WINS name server that is available to Microsoft DHCP clients.
- **netbios-node-type** - Configures the NetBIOS node type for Microsoft DHCP clients, for the corresponding DHCP server address pool.
- **default-router** - Configures the IP address of a default router to which a DHCP client should send packets after booting, for the corresponding DHCP server address pool.
- **option –** Configures, for the corresponding DHCP server address pool, the various available DHCP server options with the corresponding specific values.
- **lease** - Configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.
- **utilization threshold –** Configures pool utilization threshold value (in percentage) for the corresponding DHCP server address pool.
- **host hardware-type** - Configures host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool.
- **show ip dhcp server statistics** - Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

41.3.24 show ip dhcp server binding

This command displays the DHCP server binding information.

A DHCP binding is created when a DHCP server assigns an IP address to a DHCP client. The information contains the allocated IP address, host hardware type, host hardware address, binding state and expiry time of the allocated DHCP lease.

show ip dhcp server binding

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ip dhcp server binding

Ip          Hw          Hw                  Binding   Expire
Address     Type        Address             State     Time
--------    ----        -------             ------    ------
12.0.0.2 Ethernet 00:02:02:03:04:01 Assigned May 12 13:22:41 2009
```

☞ The DHCP server binding information is displayed, only if the DHCP server is enabled and the DHCP binding is created.

Related Commands

- **service dhcp-server** - Enables the DHCP server in the switch.
- **ip dhcp** - Enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server.
- **host hardware-type** - Configures host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool.

41.3.25 show ip dhcp server statistics

This command displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

show ip dhcp server statistics

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ip dhcp server statistics

Address pools : 2

Message                 Received
-------                 --------
DHCPDISCOVER            6
DHCPREQUEST             2
DHCPDECLINE             0
DHCPRELEASE             0
DHCPINFORM              0

Message                 Sent
-------                 ----
DHCPOFFER               6
DHCPACK                 2
DHCPNAK                 0
```

Related Commands

- **service dhcp-server** - Enables the DHCP server in the switch.
- **ip dhcp pool –** Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- **ip dhcp** - Enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server.
- **show ip dhcp server pools** - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

Chapter 42

DHCPv6

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) enables DHCP servers to pass configuration parameters such as IPv6 network addresses, to IPv6 nodes. It allows to automatically allocate reusable network addresses and provides additional configuration flexibility.

Interface Masters DHCPv6 has DHCPv6 client, DHCPv6 server and DHCPv6 relay functionalities. **Interface Masters DHCPv6** runs as an application over IPv6 and uses SLI (Socket Layer Interface) to send or receive messages from the corresponding client or server.

The list of CLI commands for the configuration of DHCPv6 is as follows

DHCP client:

- snmp-server enable traps ipv6 dhcp client
- ipv6 dhcp client port
- ipv6 dhcp client syslog
- ipv6 address dhcp
- ipv6 dhcp authentication client
- ipv6 dhcp client-id type
- ipv6 dhcp client-id interface
- ipv6 dhcp timer
- ipv6 dhcp client information refresh minimum
- debug ipv6 dhcp client
- clear ipv6 dhcp client statistics
- show ipv6 dhcp

- show ipv6 dhcp interface
- show ipv6 dhcp client statistics

DHCP relay:

- snmp-server enable traps ipv6 dhcp relay
- ipv6 dhcp relay syslog
- ipv6 dhcp relay port
- ipv6 dhcp relay
- ipv6 dhcp relay hop-threshold
- debug ipv6 dhcp relay
- clear ipv6 dhcp relay statistics
- show ipv6 dhcp
- show ipv6 dhcp interface
- show ipv6 dhcp relay statistics

DHCP server:

- snmp-server enable traps ipv6 dhcp server
- ipv6 dhcp server port
- ipv6 dhcp server syslog
- ipv6 dhcp authentication server client-id
- ipv6 dhcp authentication
- ipv6 dhcp pool
- vendor-specific
- sub option
- link-address
- domain-name
- dns-server
- sip address
- sip domain-name
- option
- ipv6 dhcp server-id type
- ipv6 dhcp server-id interface
- information refresh
- ipv6 dhcp server
- debug ipv6 dhcp server
- clear ipv6 dhcp server statistics

- show ipv6 dhcp
- show ipv6 dhcp pool
- show ipv6 dhcp interface
- show ipv6 dhcp server statistics

42.1 DHCPv6 Client

The DHCPv6 client is a node that initiates requests on a link to obtain configuration parameters (such as list of available DNS (Domain Name Server) servers) from DHCPv6 servers. It transmits and receives DHCP messages using link-local address or addresses determined through other mechanisms.

This section describes the commands required to configure and view the DHCPv6 client related parameters.

42.1.1 snmp-server enable traps ipv6 dhcp client

This command enables the SNMP traps for DHCPv6 client. It enables all the traps, when executed without any option.

The no form of the command disables the SNMP traps for the DHCPv6 client. It sets the trap as none, when executed without any option.

`snmp-server enable traps ipv6 dhcp client [invalid-pkt] [auth-fail]`

`no snmp-server enable traps ipv6 dhcp client [invalid-pkt] [auth-fail]`

Syntax Description	**`invalid-pkt`**	-	Enables or disables the transmission of invalid packet trap notification This trap notification is generated, when the received reply message is invalid.
	`auth-fail`	-	Enables or disables the transmission of HMAC authentication fail trap notification. This trap notification is generated, when the received reply message contains the authentication TLV and digest calculated at the client side that does not match with the received digest value. The digest is calculated at the client side with the realm and key ID values.
Mode	Global Configuration mode		
Package	Workgroup, Enterprise and Metro		
Defaults	SNMP traps are disabled for the DHCPv6 client (that is, no SNMP trap is configured).		
Example	`iss(config)# snmp-server enable traps ipv6 dhcp client invalid-pkt`		
☞	• This command allows to enable multiple SNMP traps for the DHCPv6 client. That is, both the specified trap notifications can be enabled one after the other.		
Related Commands	• **`show ipv6 dhcp`** – Displays the configuration information		

42.1.2 ipv6 dhcp client port

This command configures the listen or transmit UDP (User Datagram Protocol) ports.

```
ipv6 dhcp client port { listen <value (1-65535)> | transmit <value(1-65535)>}
```

Syntax Description	**listen**	-	UDP listen port number to be provided in UDP header of the information-request message. This value ranges between 1 and 65535.
	transmit	-	UDP(User Datagram Protocol) destination port number to be provided in UDP header of the information-request message. This value ranges between 1 and 65535.
Mode	Global Configuration mode		
Package	Workgroup, Enterprise and Metro		
Defaults	listen	-	546
	transmit	-	547
Example	`iss(config)# ipv6 dhcp client port listen 540`		

☞
- Client processes the received reply message, only when the destination port number in the UDP header is equal to the client listen port number.

Related Commands **`show ipv6 dhcp`** – Displays the configuration information

42.1.3 ipv6 dhcp client syslog

This command enables or disables the syslog generation.

```
ipv6 dhcp client syslog {enable | disable}
```

Syntax Description	**enable**	-	Enables the transmission of syslog notification messages. DHCPv6 client generates syslog messages.
	disable	-	Disables the transmission of syslog notification messages. DHCPv6 client does not generate any syslog messages.
Mode	Global Configuration mode		
Package	Workgroup, Enterprise and Metro		
Defaults	disable		
Example	`iss(config)# ipv6 dhcp client syslog enable`		
Related Commands	• **show ipv6 dhcp** – Displays the configuration information		

42.1.4 ipv6 address dhcp

This command enables the DHCPv6 client functionality over the interface and requests for configuration information from the client. The no form of the command disables the DHCPv6 client functionality over the interface.

ipv6 address dhcp

no ipv6 address dhcp

Mode	Interface Configuration mode
Package	Workgroup, Enterprise and Metro
Defaults	DHCPv6 client functionality is disabled
Example	`iss(config-if)# ipv6 address dhcp`

☞

- The physical interface should be configured as router port, before executing this command for the physical interface.

Related Commands

- **no switchport** – Configures the port as router port
- **ipv6 dhcp authentication client-** Defines the domain, client identifier and the corresponding authentication MD5 (Message Digest 5) keys used to authenticate the information-request message and validate reply message
- **ipv6 dhcp client-id type** – Configures the DUID type to be used for the client identifier
- **ipv6 dhcp client-id interface** – Configures the interface that is used in the formation of the DUID based on LLT or on LL
- **ipv6 dhcp timer** – Configures various timer parameters for a retransmission algorithm of the information-request message
- **ipv6 dhcp client information refresh minimum** – Sets the minimum refresh timer value for the information-request message, at the client side
- **clear ipv6 dhcp client statistics** – Clears the DHCPv6 client statistics for the specified interface or all the interfaces
- **show ipv6 dhcp interface** – Displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces
- **show ipv6 dhcp client statistics** – Displays the DHCPv6 client statistics

42.1.5 ipv6 dhcp authentication client

This command defines the domain, client identifier and the corresponding authentication MD5 (Message Digest 5) keys used to authenticate the information-request message and validate reply message.

```
ipv6 dhcp authentication client {realm <string(1-128)> | key <string (1-64)> |
keyid <value>}
```

Syntax Description

realm	-	Name of the container for the HMAC-MD5 (Hash Message Authentication Code - Message Digest 5) authentication key. This value is a string of size varying between 1 and 128.
key	-	HMAC-MD5 key string used to authenticate the information-request message. This value is a string of size varying between 1 and 64.
keyid	-	Key identifier that is transmitted in information-request message as part of authentication information. The server searches, using this key identifier, in its local database for the related key to calculate the HMAC. This value ranges between 0 and 4294967295.

Mode Interface Configuration mode

Package Workgroup, Enterprise and Metro

Defaults keyid - 1

Example

```
iss(config-if)# ipv6 dhcp authentication client realm container1
```

☞

- The physical interface should be configured as router port, before executing this command for the physical interface.
- The DHCPv6 client functionality should be enabled in the interface, before executing this command.

Related Commands

- **no switchport** – Configures the port as router port
- **ipv6 address dhcp** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- **show ipv6 dhcp interface** – Displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces

42.1.6 ipv6 dhcp client-id type

This command configures the DUID (DHCP Unique Identifier) type to be used for the client identifier.

DUID consists of a two-octet type code represented in network byte order and a variable number of octets, to make an actual identifier. This DUID is used to identify the clients.

Client sends a client identifier TLV (Type Length Value) in the information-request message.

`ipv6 dhcp client-id type {llt | en | ll}`

Syntax Description

`llt`	-	DUID is formed based on LLT (Link-Layer Address plus Time). The DHCPv6 client uses the link layer address of the interface and current system time value for the client identifier option TLV value. This type of DUID consists of a two octet type field containing the value one, a two octet hardware type code, four octets containing a time value, and a link-layer address of any one network interface that is connected to the DHCP device at the time of generation of the DUID.
`en`	-	DUID is assigned by the vendor based on EN (Enterprise Number). The DHCPv6 client uses the vendor-assigned unique ID based on the EN for the client identifier option TLV value. This type of DUID consists of vendor's registered private enterprise number as maintained by IANA (Internet Assigned Numbers Authority) and a unique identifier assigned by the vendor.
`ll`	-	DUID is formed based on LL (Link-layer Address). The DHCPv6 client uses the link layer address for the client identifier option TLV value. This type of DUID consists of two octets containing the DUID type 3, a two octet network hardware type code, and a link-layer address of any one network interface that is permanently connected to the client or server device.

Mode Interface Configuration mode

Package Workgroup, Enterprise and Metro

Defaults llt

Example

```
iss(config-if)# ipv6 dhcp client-id type ll
```

☞
- The physical interface should be configured as router port, before executing this command for the physical interface.

- The DHCPv6 client functionality should be enabled in the interface, before executing this command.
- For client ID configured as **llt**, the DHCPv6 client and server should:
  1. Compulsorily have a stable storage.
  2. Store DUID-LLT in stable storage.
  3. Continue to use DUID-LLT, even if network interface used to generate the DUID-LLT is removed.
  4. Attempt to configure the time prior to generation of DUID, if possible, and should use time source (For example, real-time clock) for generating the DUID, even if the source is not configurable prior to the generation of the DUID.
- For client ID configured as **en**:
  1. The identifier assigned by the vendor should be unique to device.
  2. The unique identifier should be assigned to the device during its manufacture itself and should be stored in a non-volatile storage.
  3. The generated DUID should be recorded in a non-erasable storage.
- For client ID configured as **ll**:
  1. DHCP-LL should not be used by clients or servers that cannot tell whether or not a network interface is permanently attached to the device on which the DHCP client is running.
  2. Same DHCP-LL should be used in configuring all network interfaces connected to the device, regardless of usage of any interface's link-layer address to generate the DUID.

Related Commands

- **`no switchport`** – Configures the port as router port
- **`ipv6 address dhcp`** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- **`show ipv6 dhcp interface`** – Displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces

42.1.7 ipv6 dhcp client-id interface

This command configures the interface that is used in the formation of the DUID based on LLT or on LL.

```
ipv6 dhcp client-id interface {<interface-type> <interface-id> }
```

Syntax Description

interface-type	- Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
interface-id	- This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.

Mode Interface Configuration mode

Package Workgroup, Enterprise and Metro

Defaults An arbitrary interface value is used.

Example

```
iss(config-if)# ipv6 dhcp client-id interface gigabitethernet 0/2
```

☞
- The physical interface should be configured as router port, before executing this command for the physical interface.
- The DHCPv6 client functionality should be enabled in the interface, before executing this command.
- The physical interface that is configured to be used in the formation of DUID should have been already configured as router port. Otherwise, this command throws an error.

Related Commands
- **no switchport** – Configures the port as router port
- **ipv6 address dhcp** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client

42.1.8 ipv6 dhcp timer

This command is used to set the various timer parameters for a retransmission algorithm of the information-request message. The no form of the command is used to reset the timer parameters to the default value.

By default, the client calculates the retransmission time for the information-request message using the following formula:

RT = IRT + RAND * IRT

Where RT - Retransmission Time

IRT - Initial Retransmission Time

RAND - Random number between -0.1 and +0.1

If the calculated RT becomes greater than the MRT (Maximum Retransmission Time), then the client calculates the RT using the following formula:

RT = MRT + RAND * MRT

Where RT - Retransmission Time

MRT - Maximum Retransmission Time

RAND - Random number between -0.1 and +0.1

```
ipv6 dhcp timer { irt <value(1-255)> | mrt <value(0-120)> | mrc <value(0-10)>
| mrd <value(0-100)>}
```

```
no ipv6 dhcp timer [( irt | mrt | mrc | mrd }]
```

Syntax Description

`irt`	-	Initial retransmission time value. This value ranges between 1 and 255 seconds.
`mrt`	-	Maximum retransmission time value. This value ranges between 0 and 120 seconds.
`mrc`	-	Maximum retransmission count value. This value ranges between 0 and 10. If MRC (Maximum Retransmission Count) is zero, client continues to transmit the information-request message until it receives a reply response. If MRC is non-zero, client terminates the information-request message exchange and considers it as fail, on transmitting the information-request message MRC time.
`mrd`	-	Maximum retransmission delay value. This value ranges between 0 and 100 seconds. If MRD (Maximum Retransmission Delay) is zero, client continues to transmit the information-request message until it receives a reply response.

If MRD is non-zero, client terminates the information-request message exchange and considers it as fail, once MRD is elapsed since the initial transmission of the message.

Mode Interface Configuration mode

Package Workgroup, Enterprise and Metro

Defaults

irt	-	1
mrt	-	120
mrc	-	0
mrd	-	0

Example

```
iss(config-if)# ipv6 dhcp timer irt 10
```

☞

- This command can be executed for the physical interface, only if the interface is configured as router port.
- DHCPv6 client functionality should be enabled in the interface, before executing this command.

Related Commands

- **`no switchport`** – Configures the port as router port
- **`ipv6 address dhcp`** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- **`show ipv6 dhcp interface`** – Displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces

42.1.9 ipv6 dhcp client information refresh minimum

This command sets the minimum refresh timer value for the information-request message, at the client side. The client once again sends information-request message to the server for acquiring configuration information, if the refresh timer is expired.

The no form of the command sets the refresh timer value to default value.

The configured minimum refresh timer value is used, if an information refresh time option sent by the server is less than the configured value.

This value ranges between 600 and 4294967295 seconds.

ipv6 dhcp client information refresh minimum <seconds value(600-4294967295)>

no ipv6 dhcp client information refresh minimum

Mode	Interface Configuration mode
Package	Workgroup, Enterprise and Metro
Defaults	86400 Seconds (24 Hours)
Example	`iss(config-if)# ipv6 dhcp client information refresh minimum 10000`

☞

- The physical interface should be configured as router port, before executing this command for the physical interface.
- The DHCPv6 client functionality should be enabled in the interface, before executing this command.

Related Commands

- **no switchport** – Configures the port as router port
- **ipv6 address dhcp** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- **show ipv6 dhcp interface** – Displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces

42.1.10 debug ipv6 dhcp client

This command sets the debug traces for the DHCPv6 client. The no form of the command resets the debug traces for the DHCPv6 client.

```
debug ipv6 dhcp client {[init-shut] [mgmt] [ctrl] [pkt] [resource] [fail]
[buffer] [critical] [all]}
```

```
no debug ipv6 dhcp client {[init-shut] [mgmt] [ctrl] [pkt] [resource] [fail]
[buffer] [critical] [all]}
```

Syntax Description

`init-shut`	-	Init and shutdown traces. These traces are used during the module initialization and shutdown, and for cases such as failure of RBTree creation and so on.
`mgmt`	-	Management traces.
`ctrl`	-	Control plane traces. These traces are used for cases such as MBSM card removal, failure of state change and so on.
`pkt`	-	Packet dump traces. These traces are used during the reception and transmission of packets.
`resource`	-	Traces related to all resources such as memory, data structure and the like. These traces are used for failure of memory allocation and so on.
`fail`	-	All failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error.
`buffer`	-	Buffer allocation / release traces.
`critical`	-	SL (Stateless)-DHCPv6 client critical traces. These traces are used for cases such as failure of RBTree addition, failure to program the hardware, and so on.

	all	-	All traces.

Mode Privileged Exec Mode / User Exec Mode

Package Workgroup, Enterprise and Metro

Defaults critical

Example

```
iss# debug ipv6 dhcp client mgmt
D6CL: Trace Option Set enable mgmt
```

42.1.11 clear ipv6 dhcp client statistics

This command clears the DHCPv6 client statistics for the specified interface or all the interfaces.

clear ipv6 dhcp client statistics [interface {vlan <VlanId(1-4094)> | <interface-type> <interface-id>}]

Syntax Description	**vlan**	- VLAN identifier. This value ranges between 1 and 4094.
	interface-type	- Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
	interface-id	- This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.
Mode	Privileged Exec Mode	
Package	Workgroup, Enterprise and Metro	
Example	`iss# clear ipv6 dhcp client statistics interface gigabitethernet 0/1`	
Related Commands	• **ipv6 address dhcp** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client • **show ipv6 dhcp client statistics** – Displays the DHCPv6 client statistics	

42.1.12 show ipv6 dhcp

This command displays the configuration information.

show ipv6 dhcp

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp

Client information:
  Listen UDP port    : 546
  Transmit UDP port  : 547
  Sys log status     : disabled
  SNMP traps         : none

Server information:
  Listen UDP port                       : 547
  Client Transmit UDP port              : 546
  Relay Transmit UDP port               : 547
  Sys log status                        : disabled
  SNMP traps                            : none

  Authentication Information:
    Client DUID : 636c69656e7431
      Realm Name  : real1
        Key Value       : 1
        Key Identifier : 74:72:69:61:6c

Relay information:
  Listen UDP port                       : 547
  Client Transmit UDP port              : 546
  Server Transmit UDP port              : 547
  Sys log status                        : disabled
  SNMP traps                            : none
```

Related Commands

- **snmp-server enable traps ipv6 dhcp client** – Enables the SNMP traps for DHCPv6 client
- **ipv6 dhcp client port** – Configures the listen or transmit UDP ports
- **ipv6 dhcp client syslog** – Enables or disables the syslog generation

42.1.13 show ipv6 dhcp interface

This command displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces.

show ipv6 dhcp interface [{vlan <VlanId(1-4094)> | <interface-type> <interface-id>}]

Syntax Description

vlan	-	VLAN identifier. This value ranges between 1 and 4094.
interface-type	-	Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
interface-id	-	This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp interface

gigabitethernet 0/3 is in client mode
  DHCPv6 unique type(DUID Type) : Link-layer Address Plus Time
  DHCPv6 unique identifier(DUID):
00010002000031b9fe8000000000000020102fffe0304
                                  01
  Minimum Refresh Time          : 86400 sec
  Current Refresh Time          : 86400 sec

  Retransmission counters:
    Maximum Ret Count : 0
    Maximum Ret Delay : 0   sec
    Maximum Ret Time  : 120 sec
    Initial Ret Time  : 1   sec
    Current Ret Time  : 0   sec

  Authentication information:
    Realm Name      : -
```

```
    Key Identifier : -
    Key value      : 1

  List of known servers:
    Address    : fe80::202:2ff:fe03:401
    DUID       : 0001000200001b5bfe8000000000000020302fffe030401
    Preference : 5
      Status Code     : (Success)-SUCCESS
      SIP domain list : Interface Masters.com
      SIP servers     : fe80::200d:88ff:fe67:6666
      DNS servers     : fe80::200d:88ff:fe67:6666
      DNS search list : Interface Masters.com
```

Related Commands

- **`ipv6 address dhcp`** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- **`ipv6 dhcp authentication client`** – Defines the domain, client identifier and the corresponding authentication MD5 (Message Digest 5) keys used to authenticate the information-request message and validate reply message
- **`ipv6 dhcp client-id type`** – Configures the DUID type to be used for the client identifier
- **`ipv6 dhcp timer`** – Configures various timer parameters for a retransmission algorithm of the information-request message
- **`ipv6 dhcp client information refresh minimum`** – Sets the minimum refresh timer value for the information-request message, at the client side

42.1.14 show ipv6 dhcp client statistics

This command displays the DHCPv6 client statistics such as number of PDUs (Protocol Data Units) transmitted / received, for the specified interface or all the interfaces.

show ipv6 dhcp client statistics [interface {vlan <VlanId(1-4094)> | <interface-type> <interface-id>}]

Syntax Description

vlan	-	VLAN identifier. This value ranges between 1 and 4094.
interface-type	-	Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
interface-id	-	This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp client statistics

gigabitethernet 0/1
  Transmitted:
   information-request : 1

  Received:
   reply        : 1
   invalid      : 0
   hmac-failure : 0

vlan 1
  Transmitted:
   information-request : 1

  Received:
   reply        : 1
   invalid      : 0
   hmac-failure : 0
```

```
iss# show ipv6 dhcp client statistics interface gigabitethernet
0/1

gigabitethernet 0/1
  Transmitted:
   information-request : 1

  Received:
   reply        : 1
   invalid      : 0
   hmac-failure : 0


iss# show ipv6 dhcp client statistics interface vlan 1

vlan 1
  Transmitted:
   information-request : 1

  Received:
   reply        : 1
   invalid      : 0
   hmac-failure : 0
```

Related Commands

- **`ipv6 address dhcp`** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- **`clear ipv6 dhcp client statistics`** – Clears the DHCPv6 client statistics for the specified interface or all the interfaces

42.2 DHCPv6 Relay

The DHCPv6 relay is an intermediate node that relays DHCP messages between the DHCPv6 clients and DHCPv6 servers on on different links.

This section describes the commands required to configure and view the DHCPv6 relay related parameters.

42.2.1 snmp-server enable traps ipv6 dhcp relay

This command enables the SNMP traps for DHCPv6 relay. It enables all the traps, when executed without any option.

The no form of the command disables the SNMP traps for the DHCPv6 relay. It sets the trap as none, when executed without any option.

```
snmp-server enable traps ipv6 dhcp relay [invalid-pkt] [max-hop-count]
```

```
no snmp-server enable traps ipv6 dhcp relay [invalid-pkt] [max-hop-count]
```

Syntax Description

`invalid-pkt`	-	Enables or disables the transmission of invalid packet trap notification. This trap notification is generated, when the received message is invalid.
`max-hop-count`	-	Enables or disables the transmission of maximum hop count trap notification. This trap notification is generated, when the relay agent is not able to add the relay header, as the received hop count value is equal to the configured maximum hop threshold limit.

Mode Global Configuration mode

Package Workgroup, Enterprise and Metro

Defaults SNMP traps are disabled for the DHCPv6 relay (that is, no SNMP trap is configured).

Example

```
iss(config)# snmp-server enable traps ipv6 dhcp relay max-hop-
count
```

- This command allows to enable multiple SNMP traps for the DHCPv6 relay. That is, both the specified trap notifications can be enabled one after the other.

Related Commands

- **`show ipv6 dhcp`** – Displays the DHCPv6 relay global configurations

42.2.2 ipv6 dhcp relay syslog

This command enables or disables the syslog feature for the DHCPv6 relay.

`ipv6 dhcp relay syslog {enable | disable}`

Syntax Description	**`enable`**	-	Enables the transmission of syslog notification messages. DHCPv6 relay generates syslog messages.
	`disable`	-	Disables the transmission of syslog notification messages. DHCPv6 relay does not generate any syslog messages.
Mode	Global Configuration mode		
Package	Workgroup, Enterprise and Metro		
Defaults	disable		
Example	`iss(config)# ipv6 dhcp relay syslog enable`		
Related Commands	• **`show ipv6 dhcp`** – Displays the DHCPv6 relay global configurations		

42.2.3 ipv6 dhcp relay port

This command sets the listen UDP port number, and client and server transmit UDP port numbers.

```
ipv6 dhcp relay port {listen <value(1-65535)> | client transmit <value(1-65535)> | server transmit <value(1-65535)>}
```

Syntax Description

listen	-	UDP port number on which the DHCPv6 relay should listen. This facilitates the DHCPv6 relay to co-exist with the DHCPv6 server which can listen on a different port. This value ranges between 1 and 65535.
client transmit	-	UDP port number on which the DHCPv6 relay sends reply message. This value ranges between 1 and 65535.
server transmit	-	UDP port number on which the DHCPv6 relay sends relay-forward message. This value ranges between 1 and 65535.

Mode Global Configuration mode

Package Workgroup, Enterprise and Metro

Defaults

listen	-	547
client transmit	-	546
server transmit	-	547

Example

```
iss(config)# ipv6 dhcp relay port listen 600
```

Related Commands

- **show ipv6 dhcp** – Displays the DHCPv6 relay global configurations

42.2.4 ipv6 dhcp relay

This command enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface. The no form of the command disables the relay feature on the interface and optionally unsets the destination server address and the outgoing interface.

ipv6 dhcp relay [destination <prefix> {link-local | <prefix Len> } [interface {Vlan <vlan-id (1-4094)> | <interface-type> <interface-id>}]]

no ipv6 dhcp relay [destination <prefix> {link-local | <prefix Len> } [interface {Vlan <vlan-id (1-4094)> | <interface-type> <interface-id>}]]

Syntax Description

prefix	-	IPv6 address of the destination DHCP server.
link-local	-	Link-local type IPv6 address.
prefix Len	-	Length of the IPv6 address to be used as prefix. This value ranges between 0 to 128.
Vlan	-	VLAN identifier. This value ranges between 1 and 4094.
interface-type	-	Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
interface-id	-	This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.

Mode Interface Configuration mode

Package Workgroup, Enterprise and Metro

Defaults DHCPv6 relay feature is disabled.

Example

```
iss(config-if)# ipv6 dhcp relay
```

☞
- The physical interface should be configured as router port, before executing this command for the physical interface.

Related Commands

- **`no switchport`** – Configures the port as router port
- **`ipv6 dhcp relay hop-threshold`** – Sets the hop threshold limit for the DHCPv6 relay packets
- **`clear ipv6 dhcp relay statistics`** – Clears DHCPv6 relay transmit and receive statistics for a particular interface or for all the interfaces
- **`show ipv6 dhcp interfcae`** – Displays the DHCPv6 relay configurations on a particular interface or all the interfaces
- **`show ipv6 dhcp relay statistics`** – Displays the DHCPv6 relay statistics on a particular interface or on all the interfaces

42.2.5 ipv6 dhcp relay hop-threshold

This command sets the hop threshold limit for the DHCPv6 relay packets. The limit represents the maximum number of hop count allowed by relay agent to pass through it. Packets are dropped at the relay agent, if the hop count in DHCP message is greater than the threshold limit.

The no form of the command resets the threshold limit to default value.

ipv6 dhcp relay hop-threshold <count>

no ipv6 dhcp relay hop-threshold

Syntax Description	**count**	-	Hop threshold limit. This value ranges between 0 and 32.
Mode	Interface Configuration mode		
Package	Workgroup, Enterprise and Metro		
Defaults	4		
Example	`iss(config-if)# ipv6 dhcp relay hop-threshold 20`		

☞

- The physical interface should be configured as router port, before executing this command for the physical interface.
- The DHCPv6 relay feature should be enabled in the interface, before executing this command.

Related Commands

- **no switchport** – Configures the port as router port
- **ipv6 dhcp relay–** Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface
- **show ipv6 dhcp interface** – Displays the DHCPv6 relay configurations on a particular interface or all the interfaces

42.2.6 debug ipv6 dhcp relay

This command sets the debug traces for the DHCPv6 relay. The no form of the command resets the debug traces for the DHCPv6 relay.

```
debug ipv6 dhcp relay {[init-shut] [mgmt] [ctrl] [pkt] [resource] [fail]
[buffer] [critical] [all]}
```

```
no debug ipv6 dhcp relay {[init-shut] [mgmt] [ctrl] [pkt] [resource] [fail]
[buffer] [critical] [all]}
```

Syntax Description

`init-shut`	-	Init and shutdown traces. These traces are used during the module initialization and shutdown, and for cases such as failure of RBTree creation and so on.
`mgmt`	-	Management traces.
`ctrl`	-	Control plane traces. These traces are used for cases such as MBSM card removal, failure of state change and so on.
`pkt`	-	Packet dump traces. These traces are used during the reception and transmission of packets.
`resource`	-	Traces related to all resources such as memory, data structure and the like. These traces are used for failure of memory allocation and so on.
`fail`	-	All failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error.
`buffer`	-	Buffer allocation / release traces.
`critical`	-	SL-DHCPv6 relay critical traces.

			These traces are used for cases such as failure of RBTree addition, failure to program the hardware, and so on.
	all	-	All traces.

Mode Privileged Exec Mode / User Exec Mode

Package Workgroup, Enterprise and Metro

Defaults critical

Example

```
iss# debug ipv6 dhcp relay mgmt
```

42.2.7 clear ipv6 dhcp relay statistics

This command clears DHCPv6 relay transmit and receive statistics for a particular interface or for all the interfaces.

clear ipv6 dhcp relay statistics [interface {vlan <VlanId(1-4094)> |<interface-type> <interface-id>}]

Syntax Description	**vlan**	-	VLAN identifier. This value ranges between 1 and 4094.
	interface-type	-	Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
	interface-id	-	This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.
Mode	Privileged Exec Mode		
Package	Workgroup, Enterprise and Metro		
Example	`iss# clear ipv6 dhcp relay statistics`		
Related Commands	• **ipv6 dhcp relay**– Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface • **show ipv6 dhcp relay statistics** – Displays the DHCPv6 relay statistics on a particular interface or on all the interfaces		

42.2.8 show ipv6 dhcp

This command displays the DHCPv6 relay global configurations.

show ipv6 dhcp

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp

Client information:
  Listen UDP port    : 546
  Transmit UDP port  : 547
  Sys log status     : disabled
  SNMP traps         : none

Server information:
  Listen UDP port                       : 547
  Client Transmit UDP port              : 546
  Relay Transmit UDP port               : 547
  Sys log status                        : disabled
  SNMP traps                            : none

  Authentication Information:
    Client DUID : 636c69656e7431
      Realm Name  : real1
        Key Value       : 1
        Key Identifier : 74:72:69:61:6c

Relay information:
  Listen UDP port                       : 547
  Client Transmit UDP port              : 546
  Server Transmit UDP port              : 547
  Sys log status                        : disabled
  SNMP traps                            : none
```

Related Commands

- **snmp-server enable traps ipv6 dhcp** – Enables the SNMP traps for DHCPv6 relay
- **ipv6 dhcp relay syslog** – Enables or disables the syslog feature for the DHCPv6 relay
- **ipv6 dhcp relay port** – Sets the listen UDP port number, and client and server transmit UDP port numbers

42.2.9 show ipv6 dhcp interface

This command displays the DHCPv6 relay configurations on a particular interface or all the interfaces.

show ipv6 dhcp interface [{vlan <VlanId(1-4094)> | <interface-type> <interface-id>}]

Syntax Description

vlan	-	VLAN identifier. This value ranges between 1 and 4094.
interface-type	-	Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
interface-id	-	This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp interface
gigabitethernet 0/4 is in relay mode
  HopThreshold value : 4
  Server Address     : unicast to configured servers only
    fe80::219:dbff:fe88:dc07 : Gi0/3
```

Related Commands

- **ipv6 dhcp relay** – Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface
- **ipv6 dhcp relay hop-threshold** – Sets the hop threshold limit for the DHCPv6 relay packets

42.2.10 show ipv6 dhcp relay statistics

This command displays the DHCPv6 relay statistics on a particular interface or on all the interfaces.

show ipv6 dhcp relay statistics [interface {vlan <VlanId(1-4094)> | <interface-type> <interface-id>}]

Syntax Description

vlan	-	VLAN identifier. This value ranges between 1 and 4094.
interface-type	-	Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
interface-id	-	This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp relay statistics

 gigabitethernet 0/4
  Received:
    information-request : 1
    relay-forward       : 0
    relay-reply         : 1
    invalid             : 0
```

Related Commands

- **ipv6 dhcp relay** – Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface
- **clear ipv6 dhcp relay statistics** – Clears DHCPv6 relay transmit and receive statistics for a particular interface or for all the interfaces

42.3 DHCPv6 Server

The DHCPv6 server is a node that responds to requests from the DHCPv6 clients. It can be on the same link as the clients or on the different link. It receives DHCP messages from the clients using a reserved, link-scoped multicast address.

This section describes the commands required to configure and view the DHCPv6 server related parameters.

42.3.1 snmp-server enable traps ipv6 dhcp server

This command enables the SNMP traps for DHCPv6 server. It enables all the traps, when executed without any option.

The no form of the command disables the SNMP traps for the DHCPv6 server. It sets the trap as none, when executed without any option.

```
snmp-server enable traps ipv6 dhcp server [unknown-tlv] [invalid-pkt] [auth-fail]
```

```
no snmp-server enable traps ipv6 dhcp server [unknown-tlv] | [invalid-pkt] | [auth-fail]
```

Syntax Description

`unknown-tlv`	-	Enables or disables the transmission of unknown TLV trap notification . This trap notification is generated, when received information-request or relay forward message contains invalid TLV type.
`invalid-pkt`	-	Enables or disables the transmission of invalid packet trap notification This trap notification is generated, when the received information-request or relay forward message is invalid.
`auth-fail`	-	Enables or disables the transmission of HMAC authentication fail trap notification. This trap notification is generated, when the received information-request or relay forward message contains the authentication TLV and digest calculated at the server side that does not match with the received digest value. The digest is calculated at the server side with the realm and key ID values.

Mode Global Configuration mode

Package Workgroup, Enterprise and Metro

Defaults SNMP traps are disabled for the DHCPv6 server (that is, no SNMP trap is configured).

Example

```
iss(config)# snmp-server enable traps ipv6 dhcp server invalid-
pkt
```

☞

- This command allows to enable multiple SNMP traps for the DHCPv6 client. That is, all the three specified trap notifications can be enabled one after the other.

Related Commands

- **`show ipv6 dhcp`** – Displays the various configuration information at server end

42.3.2 ipv6 dhcp server port

This command configures the information-request listen, reply transmit and relay-reply transmit UDP ports.

```
ipv6 dhcp server port {listen <value(1-65535)> | client transmit <value(1-65535)> | relay transmit <value(1-65535)>}
```

Syntax Description

`listen`	-	UDP listen port number. This value ranges between 1 and 65535.	
		.	Server processes the received information - request message and relay forward message, only if destination port number in UDP header is equal to the configured listen port number.
`client transmit`	-	UDP transmit port, which is set as the destination port number in UDP header of the reply message. This value ranges between 1 and 65535.	
`relay transmit`	-	UDP transmit port, which is set as the destination port number in UDP header of the relay-reply message. This value ranges between 1 and 65535.	

Mode Global Configuration mode

Package Workgroup, Enterprise and Metro

Defaults

listen	-	547
client transmit	-	546
relay transmit	-	547

Example

```
iss(config)# ipv6 dhcp server port listen 800
```

Related Commands

- **`show ipv6 dhcp`** – Displays the various configuration information at server end

42.3.3 ipv6 dhcp server syslog

This command enables or disables the syslog feature in DHCPv6 server.

ipv6 dhcp server syslog {enable | disable}

Syntax Description	**enable**	-	Enables the transmission of syslog notification messages. DHCPv6 server generates syslog messages.
	disable	-	Disables the transmission of syslog notification messages. DHCPv6 server does not generate any syslog messages.
Mode	Global Configuration mode		
Package	Workgroup, Enterprise and Metro		
Defaults	disable		
Example	`iss(config)# ipv6 dhcp server syslog enable`		
Related Commands	• **show ipv6 dhcp** – Displays the various configuration information at server end		

42.3.4 ipv6 dhcp authentication server client-id

This command creates client configuration pool at the server and enters into the client information configuration mode. It allows to create multiple client configuration pools at the server.

The no form of the command deletes the client configuration pool maintained at the server.

```
ipv6 dhcp authentication server client-id <string(128)> {llt | en | ll}
```

```
no ipv6 dhcp authentication server client-id string(1-128)
```

Syntax Description

`string`	-	Name of the client. This value is a string of size varying between 1 and 128.
`llt`	-	DUID is formed based on LLT (Link-Layer Address plus Time). The DHCPv6 client uses the link layer address of the interface and current system time value for the client identifier option TLV value. This type of DUID consists of a two octet type field containing the value 1, a two octet hardware type code, four octets containing a time value, and a link-layer address of any one network interface that is connected to the DHCP device at the time of generation of the DUID.
`en`	-	DUID is assigned by the vendor based on EN. The DHCPv6 client uses the vendor-assigned unique ID based on the EN for the client identifier option TLV value. This type of DUID consists of vendor's registered private enterprise number as maintained by IANA and a unique identifier assigned by the vendor.
`ll`	-	DUID is formed based on LL (Link-layer Address). The DHCPv6 client uses the link layer address for the client identifier option TLV value. This type of DUID consists of two octets containing the DUID type 3, a two octet network hardware type code, and a link-layer address of any one network interface that is permanently connected to the client or server device.

Mode Global Configuration mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config)# ipv6 dhcp authentication server client-id client1 en
```

☞

- For client ID configured as **llt**, the DHCPv6 client and server should:
  1. Compulsorily have a stable storage.
  2. Store DUID-LLT in stable storage.
  3. Continue to use DUID-LLT, even if network interface used to generate the DUID-LLT is removed.
  4. Attempt to configure the time prior to generation of DUID, if possible, and should use time source (For example, real-time clock) for generating the DUID, even if the source is not configurable prior to the generation of the DUID.
- For client ID configured as **en**:
  1. The identifier assigned by the vendor should be unique to device.
  2. The unique identifier should be assigned to the device during its manufacture itself and should be stored in a non-volatile storage.
  3. The generated DUID should be recorded in a non-erasable storage.
- For client ID configured as **ll**:
  1. DHCP-LL should not be used by clients or servers that cannot tell whether or not a network interface is permanently attached to the device on which the DHCP client is running.
  2. Same DHCP-LL should be used in configuring all network interfaces connected to the device, regardless of usage of any interface's link-layer address to generate the DUID.

Related Commands

- **`ipv6 dhcp authentication`** – Configures the realm and key value
- **`show ipv6 dhcp`** – Displays the various configuration information at server end

42.3.5 ipv6 dhcp authentication

This command configures the realm and key value. The no form of the command deletes the realm and key value.

```
ipv6 dhcp authentication realm <string (1-128)> key <string(1-64)>

no ipv6 dhcp authentication server realm <string (1-128)> [key <string(1-64)>
]
```

Syntax Description	**realm**	-	Name of the container used to store the HMAC-MD5 authentication keys. This value is a string of size varying between 8 and 128.
	key	-	HMAC-MD5 key string used to authenticate the information-request message. This value is a string of size varying between 8 and 64.
Mode	Client Information Configuration mode		
Package	Workgroup, Enterprise and Metro		
Example	`iss(config-d6clnt)# ipv6 dhcp authentication realm real1 key Interface Masters123`		

☞
- The client configuration pool should be created, before configuring the realm and key value.
- When this command is executed for next client ID with the same container name, the key-identifier and key value of the previous client-ID is inherited to the new client ID and then the concerned key identifier and key value are assigned to the new client ID based on the configuration.

Related Commands
- **ipv6 dhcp authentication server client-id** – Creates client configuration pool at the server and enters into the client pool configuration mode
- **show ipv6 dhcp** – Displays the various configuration information at server end

42.3.6 ipv6 dhcp pool

This command creates a DHCP6 server pool and enters into IPv6 DHCP pool configuration mode. The no form of the command deletes the DHCP6 server pool.

ipv6 dhcp pool <string (1-64)>

no ip dhcp pool <string (1-64)>

Syntax Description	**string**	-	Configuration pool name. This string size varies between 1 and 64.
		.	This name should be a unique and NULL terminated string.

Mode Global Configuration mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config)# ipv6 dhcp pool dhcp6pool1
```

Related Commands

- **`vendor-specific`** – Enters into vendor-specific configuration mode with vendor-specific identification number
- **`sub option`** – Enables a sub-option of the configured vendor specific information
- **`link-address`** – Sets a link-address IPv6 prefix
- **`domain-name`** – Defines the DNS domain suffix which is provided to the client in reply message on request
- **`dns-server`** – Defines the DNS server IP address which is provided to the client in reply message on request
- **`sip address`** – Defines the SIP server IP address which is provided to the client in reply message on request
- **`sip domain-name`** – Defines the SIP domain name which is provided to the client in reply message on request
- **`option`** – Sets pool specific DHCP6 server option
- **`ipv6 dhcp server-id type`** – Configures the DUID type to be used for the server identifier
- **`ipv6 dhcp server-id interface`** – Configure the interface that is used in the formation of the DUID based on LLT or on LL
- **`information refresh`** – Configures the refresh time value that is to be sent to the client
- **`show ipv6 dhcp pool`** – Displays the DHCPv6 server pool information
- **`show ipv6 dhcp interface`** – Displays the various configuration information at server end for specified interface or all the interfaces

42.3.7 vendor-specific

This command enters into vendor-specific configuration mode with vendor-specific identification number. The no form of the command deletes all configured vendor specific information.

vendor-specific <vendor-id (1-2147483647)>

no vendor-specific <vendor-id (1-2147483647)>

Syntax Description	**vendor-id**	-	Vendor identifier. This value ranges between 1 and 2147483647.

Mode IPv6 DHCP Pool Configuration mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config-d6pool)# vendor-specific 10
```

☞

- The DHCPv6 server address pool should be created, before configuring the vendor specific information.

Related Commands

- **ipv6 dhcp pool** – Creates a DHCP6 server address pool
- **sub option** – Enables a sub-option of the configured vendor specific information
- **show ipv6 dhcp pool** – Displays the DHCPv6 server pool information

42.3.8 sub option

This command enables a sub-option of the configured vendor specific information. The no form of the command deletes the sub-option.

```
sub option <option-id (1-4294967295)> { address <IPv6-address> | ascii <ASCII-string> | hex <hex_string>}
```

```
no sub option <option-id> { address <IPv6-address> | ascii <ASCII-string> | hex <hex_string>}
```

Syntax Description

option-id	-	Indicates a unique sub-option type. This value ranges between 1 and 4294967295.
address	-	An IPv6 address that can be provided as a sub-option value.
ascii	-	An ASCII string that can be provided as a sub-option value. This value is a string of size varying between 1 and 255.
hex	-	A hexadecimal string that can be provided as a sub-option value. This value is an octet string of size varying between 1 and 32.

Mode Vendor Specific Information Configuration mode

Package Workgroup, Enterprise and Metro

Example

```
iss(d6pool-vendor)# sub option 10 ascii 10
```

☞

- The DHCPv6 server address pool should be created and the vendor-specific information should be configured, before enabling sub-option of the vendor specific information.

Related Commands

- **ipv6 dhcp pool** – Creates a DHCP6 server address pool
- **vendor-specific** – Enters into vendor-specific configuration mode with vendor-specific identification number

42.3.9 link-address

This command sets a link-address IPv6 prefix. The server uses the configuration information pool, when an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix.

The no form of the command removes the link-address IPv6 prefix.

```
link-address <IPV6-Prefix>
```

```
no link-address <IPV6-Prefix>
```

Syntax Description	**IPV6-Prefix**	-	IPv6 address.
Mode	IPv6 DHCP Pool Configuration mode		
Package	Workgroup, Enterprise and Metro		
Example	`iss(config-d6pool)# link-address 2222::1111`		

☞
- The DHCPv6 server address pool should be created, before executing this command.

Related Commands

- **`ipv6 dhcp pool`**– Creates a DHCP6 server address pool
- **`show ipv6 dhcp pool`**– Displays the DHCPv6 server pool information

42.3.10 domain-name

This command defines the DNS domain suffix which is provided to the client in reply message on request. The no form of the command deletes the DNS domain suffix.

```
domain-name <domain name> [preference <value (0-255)> ]

no domain-name <domain name> [preference value]
```

Syntax Description	**domain name**	-	Domain name prefix that is used to resolve a domain name. This value is a string of size varying between 1 and 64.
	preference	-	Preference value of the pool. This value ranges between 0 and 255. The DHCPv6 client uses this value to select the best information on receiving multiple reply messages from different servers.

Mode IPv6 DHCP Pool Configuration mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config-d6pool)# domain-name dns1
```

☞
- The DHCPv6 server address pool should be created, before executing this command.

Related Commands
- **ipv6 dhcp pool**– Creates a DHCP6 server address pool
- **show ipv6 dhcp pool** – Displays the DHCPv6 server pool information

42.3.11 dns-server

This command defines the DNS server IP address which is provided to the client in reply message on request. The no form of the command deletes the DNS server IP address.

dns-server <ipv6-address>

no dns-server <ipv6-address>

Syntax Description	**ipv6-address**	-	IPv6 address of the DNS recursive server.
Mode	IPv6 DHCP Pool Configuration mode		
Package	Workgroup, Enterprise and Metro		
Example	`iss(config-d6pool)# dns-server 3333::2222`		

☞
- The DHCPv6 server address pool should be created, before executing this command.

Related Commands
- **ipv6 dhcp pool** – Creates a DHCP6 server address pool
- **show ipv6 dhcp pool** – Displays the DHCPv6 server pool information

42.3.12 sip address

This command defines the SIP server IP address which is provided to the client in reply message on request. The no form of the command deletes the SIP server IP address.

```
sip address <ipv6-address> [preference <value (0-255)> ]
```

```
no sip address <ipv6-address>
```

Syntax Description	**ipv6-address**	-	IPv6 address of the SIP server
	preference	-	Preference value of the pool. This value ranges between 0 and 255. The DHCPv6 client uses this value to select the best information on receiving multiple reply messages from different servers.

Mode IPv6 DHCP Pool Configuration mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config-d6pool)# sip address 4444::1111
```

☞
- The DHCPv6 server address pool should be created, before executing this command.

Related Commands

- **ipv6 dhcp pool** – Creates a DHCP6 server address pool
- **show ipv6 dhcp pool** – Displays the DHCPv6 server pool information

42.3.13 sip domain-name

This command defines the SIP domain name which is provided to the client in reply message on request. The no form of the command deletes the SIP domain name.

sip domain-name <domain-name>

no sip domain-name <domain-name>

Syntax Description	**domain-name**	-	Domain name of the SIP server
Mode	IPv6 DHCP Pool Configuration mode		
Package	Workgroup, Enterprise and Metro		
Example	`iss(config-d6pool)# sip domain-name sip1`		

☞
- The DHCPv6 server address pool should be created, before executing this command.

Related Commands
- **ipv6 dhcp pool** – Creates a DHCP6 server address pool
- **show ipv6 dhcp pool** – Displays the DHCPv6 server pool information

42.3.14 option

This command sets pool specific DHCP6 server option. The no form of the command deletes the pool specific DHCP6 server option.

```
option <code (1-65535)> { ascii <string> | hex <Hex String> | ipv6 <address> }

no option <code (1-65535)> { ascii <string> |hex <hex_str> | ipv6 <address> }
```

Syntax Description

code	-	Indicates a unique option type. This value ranges between 1 and 65535.
ascii	-	An ASCII string that can be provided as an option value. This value is a string of size varying between 1 and 255.
hex	-	A hexadecimal string that can be provided as an option value. This value is an octet string of size varying between 1 and 32.
address	-	An IPv6 address that can be provided as an option value.

Mode IPv6 DHCP Pool Configuration mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config-d6pool)# option 30 ipv6 2222::1111
```

☞

- The DHCPv6 server address pool should be created, before executing this command.

Related Commands

- **ipv6 dhcp pool** – Creates a DHCP6 server address pool
- **show ipv6 dhcp pool** – Displays the DHCPv6 server pool information

42.3.15 ipv6 dhcp server-id type

This command configures the DUID type to be used for the server identifier.

DUID consists of a two-octet type code represented in network byte order and a variable number of octets, to make an actual identifier.

Server sends a server identifier TLV in the reply message.

ipv6 dhcp server-id type {llt | en | ll}

Syntax Description

llt	- DUID is formed based on LLT. The DHCPv6 server uses the link layer address of the interface and current system time value for the server identifier option TLV value. This type of DUID consists of a two octet type field containing the value 1, a two octet hardware type code, four octets containing a time value, and a link-layer address of any one network interface that is connected to the DHCP device at the time of generation of the DUID.
en	- DUID is assigned by the vendor based on EN. The DHCPv6 server uses the vendor-assigned unique ID based on the EN for the server identifier option TLV value. This type of DUID consists of vendor's registered private enterprise number as maintained by IANA and a unique identifier assigned by the vendor.
ll	- DUID is formed based on LL. The DHCPv6 server uses the link layer address for the server identifier option TLV value. This type of DUID consists of two octets containing the DUID type 3, a two octet network hardware type code, and a link-layer address of any one network interface that is permanently connected to the client or server device.

Mode IPv6 DHCP Pool Configuration mode

Package Workgroup, Enterprise and Metro

Defaults llt

Example

```
iss(config-d6pool)# ipv6 dhcp server-id type en
```

- The DHCPv6 server address pool should be created, before executing this command.
- For server ID configured as **llt**, the DHCPv6 client and server should:
  1. Compulsorily have a stable storage.
  2. Store DUID-LLT in stable storage.
  3. Continue to use DUID-LLT, even if network interface used to generate the DUID-LLT is removed.
  4. Attempt to configure the time prior to generation of DUID, if possible, and should use time source (For example, real-time clock) for generating the DUID, even if the source is not configurable prior to the generation of the DUID.
- For server ID configured as **en**:
  1. The identifier assigned by the vendor should be unique to device.
  2. The unique identifier should be assigned to the device during its manufacture itself and should be stored in a non-volatile storage.
  3. The generated DUID should be recorded in a non-erasable storage.
- For server ID configured as **ll**:
  1. DHCP-LL should not be used by clients or servers that cannot tell whether or not a network interface is permanently attached to the device on which the DHCP client is running.
  2. Same DHCP-LL should be used in configuring all network interfaces connected to the device, regardless of usage of any interface's link-layer address to generate the DUID.

Related Commands

- **`ipv6 dhcp pool`** – Creates a DHCP6 server address pool
- **`show ipv6 dhcp pool`** – Displays the DHCPv6 server pool information

42.3.16 ipv6 dhcp server-id interface

This command is used to configure the interface that is used in the formation of the DUID based on LLT or on LL.

`ipv6 dhcp server-id interface <interface-type> <interface-id>`

Syntax Description	**`interface-type`**	- Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
	`interface-id`	- This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.
Mode	IPv6 DHCP Pool Configuration mode	
Package	Workgroup, Enterprise and Metro	
Defaults	An arbitrary interface value is used.	
Example	`iss(config-d6pool)# ipv6 dhcp server-id interface gi 0/3`	
☞	• The DHCPv6 server address pool should be created, before executing this command. • The physical interface that is configured to be used in the formation of DUID should have been already configured as router port. Otherwise, this command throws an error.	
Related Commands	• **`ipv6 dhcp pool`** – Creates a DHCP6 server address pool	

42.3.17 information refresh

This command configures the refresh time value that is to be sent to the client. The minimum refresh time value that is to be set is 600 seconds (10 minutes).

The no form of the command deletes the refresh timer option from the pool.

```
information refresh {days < value integer(0-7) > [hours < value integer(0-24)>
minutes(0-60) < value integer> ] | infinity}
```

```
no information refresh
```

Syntax Description	**days**	-	Refresh time is specified in number of days.
	hours	-	Refresh time is specified in number of hours.
	minutes	-	Refresh time is specified in number of minutes.
	infinity	-	Sets IPv6 value of 0xffffffff that is used to configure the information refresh time to infinity. That is, sets the refresh time value as 4294967295 seconds.

Mode IPv6 DHCP Pool Configuration mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config-d6pool)# information refresh days 0 hours 0 minutes 10
```

☞

- The DHCPv6 server address pool should be created, before executing this command.

Related Commands

- **ipv6 dhcp pool** – Creates a DHCP6 server address pool
- **show ipv6 dhcp pool** – Displays the DHCPv6 server pool information

42.3.18 ipv6 dhcp server

This command associates the DHCPv6 server pool with an interface. The no form of the command removes the associaton of the server pool with the interface.

ipv6 dhcp server [<pool-name (1-64)> [preference <value (0-255)>]]

no ipv6 dhcp server

Syntax Description

pool-name	-	Configuration pool name. This string size varies between 1 and 64. . This name should be a unique and NULL terminated string.
preference	-	Preference value of the pool. This value ranges between 0 and 255. The DHCPv6 client uses this value to select the best information on receiving multiple reply messages from different servers.

Mode Interface Configuration mode

Package Workgroup, Enterprise and Metro

Defaults preference - 0

Example

```
iss(config-if)# ipv6 dhcp server dhcp6pool1 preference 1
```

☞

- The physical interface should be configured as router port, before executing this command for the physical interface.

Related Commands

- **no switchport** – Configures the port as router port
- **clear ipv6 dhcp server statistics** – Clears DHCPv6 server statistics for a particular interface or for all the interfaces
- **show ipv6 dhcp pool** – Displays the DHCPv6 server pool information
- **show ipv6 dhcp interface** – Displays the various configuration information at server end for specified interface or all the interfaces
- **show ipv6 dhcp server ststistics** – Displays the DHCPv6 server statistics

42.3.19 debug ipv6 dhcp server

This command sets the debugging options and traces in the DHCPv6 server. The no form of the command unsets the debugging options and traces in the DHCPv6 server, and resets the trace to the default value.

```
debug ipv6 dhcp server {[init-shut] [mgmt] [ctrl] [pkt] [resource] [fail]
[buffer] [critical] [all]}
```

```
no debug ipv6 dhcp server {[init-shut] [mgmt] [ctrl] [pkt] [resource] [fail]
[buffer] [critical] [all]}
```

Syntax Description

`init-shut`	-	Init and shutdown traces. These traces are used during the module initialization and shutdown, and for cases such as failure of RBTree creation and so on.
`mgmt`	-	Management traces.
`ctrl`	-	Control plane traces. These traces are used for cases such as MBSM card removal, failure of state change and so on.
`pkt`	-	Packet dump traces. These traces are used during the reception and transmission of packets.
`resource`	-	Traces related to all resources such as memory, data structure and the like. These traces are used for failure of memory allocation and so on.
`fail`	-	All failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error.
`buffer`	-	Buffer allocation / release traces.

critical	-	SL-DHCPv6 server critical traces. These traces are used for cases such as failure of RBTree addition, failure to program the hardware, and so on.
all	-	All traces.

Mode Privileged Exec Mode / User Exec Mode

Package Workgroup, Enterprise and Metro

Defaults critical

Example

```
iss# debug ipv6 dhcp server mgmt
D6SR: Trace Option Set enable mgmt
```

42.3.20 clear ipv6 dhcp server statistics

This command clears DHCPv6 server statistics for a particular interface or for all the interfaces.

clear ipv6 dhcp server statistics [interface {vlan <VlanId(1-4094)> | <interface-type> <interface-id>}]

Syntax Description

vlan	-	VLAN identifier. This value ranges between 1 and 4094.
interface-type	-	Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
interface-id	-	This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# clear ipv6 dhcp server statistics
```

Related Commands

- **ipv6 dhcp server** – Associates the DHCPv6 server pool with an interface
- **show ipv6 dhcp server ststistics** – Displays the DHCPv6 server statistics

42.3.21 show ipv6 dhcp

This command displays the various configuration information at server end.

show ipv6 dhcp

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp

Client information:
  Listen UDP port   : 546
  Transmit UDP port : 547
  Sys log status    : disabled
  SNMP traps        : none

Server information:
  Listen UDP port                      : 547
  Client Transmit UDP port             : 546
  Relay Transmit UDP port              : 547
  Sys log status                       : disabled
  SNMP traps                           : none

  Authentication Information:
    Client DUID : 636c69656e7431
      Realm Name  : real1
        Key Value      : 1
        Key Identifier : 74:72:69:61:6c

Relay information:
  Listen UDP port                      : 547
  Client Transmit UDP port             : 546
  Server Transmit UDP port             : 547
  Sys log status                       : disabled
  SNMP traps                           : none
```

Related Commands

- **snmp-server enable traps ipv6 dhcp server** – Enables the SNMP traps for DHCPv6 server
- **ipv6 dhcp server port** – Configures the information-request listen, reply transmit and relay-reply transmit UDP ports
- **ipv6 dhcp server syslog** – Enables or disables the syslog feature in DHCPv6 server
- **ipv6 dhcp authentication server client-id** – Creates client configuration pool at the server and enters into the client pool configuration mode
- **ipv6 dhcp authentication** – Configures the realm and key value

42.3.22 show ipv6 dhcp pool

This command displays the DHCPv6 server pool information.

show ipv6 dhcp pool [<pool-name(1-64)>]

Syntax Description

pool-name	-	Configuration pool name. This string size varies between 1 and 64.
	.	This name should be a unique and NULL terminated string.

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp pool server-pool1

Pool : server-pool1
  ACTIVE

  DHCPv6 unique type(DUID Type) : Link-layer Address Plus Time
  DHCPv6 unique identifier(DUID):
0001000200000167fe800000000000020102ff
                                  fe030401
  Preference             : 255
  Associated Interfaces  : Gi0/3
  Associated IPv6 Prefix :

    SIP servers     : fe80::200d:88ff:fe67:6666
    DNS servers     : fe80::200d:88ff:fe67:6666
    SIP domain list : Interface Masters.com
    DNS search list : Interface Masters.com
```

Related Commands

- **ipv6 dhcp pool** – Creates a DHCP6 server address pool
- **vendor-specific** – Enters into vendor-specific configuration mode with vendor-specific identification number
- **link-address** – Sets a link-address IPv6 prefix
- **domain-name** – Defines the DNS domain suffix which is provided to the client in reply message on request
- **dns-server** – Defines the DNS server IP address which is provided to the client in reply message on request
- **sip address** – Defines the SIP server IP address which is provided to the client in reply message on request
- **sip domain-name** – Defines the SIP domain name which is provided to the client in reply message on request
- **option** – Sets pool specific DHCP6 server option

- **`ipv6 dhcp server-id type`** – Configures the DUID type to be used for the server identifier
- **`information refresh`** – Configures the refresh time value that is to be sent to the client

42.3.23 show ipv6 dhcp interface

This command displays the various configuration information at server end for specified interface or all the interfaces.

show ipv6 dhcp interface [{vlan <VlanId(1-4094)> | <interface-type> <interface-id>}]

Syntax Description

vlan	-	VLAN identifier. This value ranges between 1 and 4094.
interface-type	-	Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
interface-id	-	This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp interface
gigabitethernet 0/3 is in server mode
  Preference value : 255
  Using pool       : server-pool1
```

Related Commands

- **ipv6 dhcp pool** – Creates a DHCP6 server address pool
- **ipv6 dhcp server** – Associates the DHCPv6 server pool with an interface

42.3.24 show ipv6 dhcp server statistics

This command displays the DHCPv6 server statistics such as numbe of PDUs transmitted or received.

show ipv6 dhcp server statistics [interface {vlan <VlanId(1-4094)> | <interface-type> <interface-id>}]

Syntax Description

vlan	- VLAN identifier. This value ranges between 1 and 4094.
interface-type	- Type of interface. This can be: • FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture which supports data transfer of 100 Megabits per second. • GigabitEthernet - A version of LAN standard architecture which supports data transfer of 1 Gigabit per second.
interface-id	- This is a combination of both slot number and port number separated by a slash. For example, 1 / 4.

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ipv6 dhcp server statistics

 gigabitethernet 0/3
  Transmitted:
    reply       : 1
    relay-reply : 0

  Received:
    information-request : 1
    relay-forward       : 0
    invalid             : 0
    hmac-failure        : 0
    lastUnknownTlv      : 0
```

Related Commands

- **ipv6 dhcp server** – Associates the DHCPv6 server pool with an interface
- **clear ipv6 dhcp server statistics** – Clears DHCPv6 server statistics for a particular interface or for all the interfaces

Chapter 43

RIP

RIP (Routing Information Protocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs. RIP is classified by the Internet Engineering Task Force (IETF) as one of several internal gateway protocols (Interior Gateway Protocol).

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination.

☞ The list of CLI commands for the configuration of RIP is common to both **Single Instance and Multiple Instance** except for a difference in the prompt that appears for the Switch with Multiple Instance support.

The prompt for the **Global Configuration Mod**e is,

```
iss(config)#
```

☞ The **parameters** specific to Multiple Instance are stated so, against the respective parameter descriptions in this document.

The output of the **Show commands** differ for Single Instance and Multiple Instance. Hence both the output are documented while depicting the show command examples.

The list of CLI commands for the configuration of RIP is as follows:

- router rip
- ip rip security
- ip rip retransmission
- network
- neighbor
- passive-interface vlan
- output-delay
- redistribute
- distribute-list route-map
- default-metric
- distance
- auto-summary - enable | disable
- ip rip default route originate
- ip rip summary-address
- ip rip default route install
- ip rip send version
- ip rip receive version
- ip rip authentication mode
- timers basic - update-value
- ip split-horizon
- debug ip rip
- show ip rip

43.1 router rip

This command enables RIP for a specific VRF instance and enters the router configuration mode. The no form of the command disables RIP on all the interfaces for a specific VRF instance. The default instance is used, if the VRF name is not specified.

router rip [vrf <name>]

no router rip [vrf <name>]

Syntax Description	**vrf**	-	Name of the VRF instance. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
Mode	Global Configuration Mode		
Package	Enterprise and Metro		
Defaults	vrf	-	default
Example	`iss(config)# router rip`		

☞ VRF instance should be created, before executing this command to enable the RIP in the context.

Related Commands

- **ip vrf** - Creates VRF instance
- **network** – Enables RIP on an IP network
- **redistribute** – Enables redistribution of corresponding protocol routes into RIP
- **distribute-list route-map** - Enables route map filtering for inbound or outbound routes
- **distance –** Enables the administrative distance of the routing protocol and sets the administrative distance value
- **show ip rip** – Displays IP RIP protocol database or statistics

43.2 ip rip security

This command accepts/ignores RIP1 packets when authentication is in use and the no form of the command sets the security level to its default value.

ip rip security { minimum | maximum }

no ip rip security

Syntax Description	**minimum**	-	Denotes that the RIP1 packets will be accepted even when authentication is in use
	maximum	-	Denotes that the RIP1 packets will be ignored when authentication is in use

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults maximum

Example
```
iss(config-router)# ip rip security minimum
```

Related Command **show ip rip** – Displays IP RIP protocol database or statistics

43.3 ip rip retransmission

This command configures the timeout interval and number of retries to retransmit the update request packet or an unacknowledged update response packet and the no form of the command sets the retransmission timeout interval or the number of retransmission retries to its default value.

ip rip retransmission { interval <timeout-value (5-10)> | retries <value (10-40)> }

no ip rip retransmit { interval | retries }

Syntax Description	**interval**	-	The timeout interval to be used to retransmit the Update request packet or an unacknowledged update response packet
	retries	-	The maximum number of retransmissions of the update request and update response packets
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults	Interval	-	5
	Retries	-	36
Example	`iss(config-router)# ip rip retransmission interval 6`		

☞ During retries, if no response is received then the routes through the next hop router are marked unreachable.

Related Command

- **show ip rip** – Displays IP RIP protocol database or statistics

43.4 network

This command enables RIP on an IP network or an unnumbered interface and the no form of the command disables RIP on an IP network or an unnumbered interface.

network <ip-address>[unnum {vlan <integer(1-4094)> [switch <switch-name>] | <iftype> <ifnum>}]

no network <ip-address> [unnum {vlan <integer(1-4094)> [switch <switch-name>] | <iftype> <ifnum>}]

Syntax Description

ip-address	-	IP address for the entry
unnum vlan	-	VLAN ID for which no IP address is configured. This value ranges between 1 and 4094.
switch	-	Switch instance / Virtual switch. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
iftype	-	Interface Type
ifnum	-	Interface ID

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# network 10.0.0.1
```

☞

- The network number specified must not contain any subnet information. RIP routing updates will be sent and received only through interfaces on this network
- RIP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update
- The IP address (network address) for the entry should be same as that of the configured interface.
- The IPv4 address should be set for the interface, only after creating and mapping the VRF instance, for enabling RIP in the VRF instance.

Related Commands

- **router rip** – Enables RIP for a specific VRF instance
- **show ip rip** – Displays IP RIP protocol database or statistics

43.5 neighbor

This command adds a trusted neighbor router and the no form of the command deletes a trusted neighbor router.

neighbor <ip address>

no neighbor <ip address>

Syntax Description	**ip-address**	-	IP address of the trusted neighbor router
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# neighbor 10.0.0.5`		

☞

- This command is used to configure the IP address of the Router from which this router can accept RIP Packets
- Multiple neighbor commands can be used to specify additional trusted neighbors or peers

Related Command

- **show ip rip** – Displays IP RIP protocol database or statistics

43.6 passive-interface vlan

This command suppresses routing updates on an interface. The no form of the command does not suppress routing updates from an interface.

passive-interface {vlan <vlan-id(1-4094)> [switch <switch-name>] | <interface-type> <interface-id>}

no passive-interface {vlan <vlan-id(1-4094)> [switch <switch-name>] | <interface-type> <interface-id>}

Syntax Description	**vlan**	-	VLAN Identifier. This value ranges between 1 and 4094.
	switch	-	Switch instance / Virtual switch. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
	<interface-type> <interface-id>	-	Interface Type and ID
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# passive-interface vlan 1`		

☞

- RIP should be enabled, before executing this command.
- If the sending of routing updates is disabled on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

Related Command

- **network** – Enables RIP on an IP network
- **show ip rip –** Displays IP RIP protocol database or statistics

43.7 output-delay

This command enables interpacket delay for RIP updates and the no form of the command disables interpacket delay for RIP updates. This command also helps in preventing the routing table from losing information by enabling the interpacket delay.

output-delay

no output-delay

Mode	Router Configuration Mode
Package	Enterprise and Metro
Example	`iss(config-router)# output-delay`

Related Command

- **show ip rip** – Displays IP RIP protocol database or statistics
- **show ip protocols** - Displays information about the active routing protocol process

43.8 redistribute

This command enables redistribution of corresponding protocol routes into RIP. The redistribution is done after applying the route map, if the route map is specified. The no form of the command disables redistribution of corresponding protocol routes into RIP. The route map is disassociated for redistribution, if the no form of the command specifies the route map.

```
redistribute { all | bgp | connected | ospf | static } [route-map <name(1-20)>]
```

```
no redistribute { all | bgp | connected | ospf | static } [route-map <name(1-20)>]
```

Syntax Description

all	-	Advertises all routes learnt in the RIP process
bgp	-	Advertises routes learnt by BGP in the RIP process
connected	-	Connected routes redistribution
ospf	-	Advertises routes learnt by OSPF in the RIP process
static	-	Statically configured routes to advertise in the RIP process
route-map	-	Name of the Route Map to be applied during redistribution of routes from Route Table Manager to RIP. If this is not specified, all routes are redistributed. This value is a string of size 20

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# redistribute all
```

☞ RIP should be enabled, before executing this command.

Related Commands

- **router rip** – Enables RIP for a specific VRF instance
- **default-metric** – Sets the RIP default metric
- **show ip rip** – Displays IP RIP protocol database or statistics

43.9 distribute-list route-map

This command enables route map filtering for inbound or outbound routes. The no form of the command disables route map filtering for inbound or outbound routes

```
distribute-list route-map <name(1-20)> {in | out}
```

```
no distribute-list route-map <name(1-20)> {in | out}
```

Syntax Description	**name**	-	Specifies the name of the Route Map for which filtering should be enabled. This value is a string of size 20.
	in	-	Sets filtering for inbound routes.
	out	-	Sets filtering for outbound routes.

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# distribute-list route-map rmap-test in
```

☞

- RIP should be enabled, before executing this command.
- Only one route map can be set for inbound or outbound routes. Another route map can be assigned, only if the already assigned route map is disabled.

Related Commands

- **router rip** – Enables RIP for a specific VRF instance

43.10 default-metric

This command sets the metric to be used for redistributed routes and the no form of the command sets the metric used with redistributed routes to its default value. The metric value[1] ranges between 1 and 16.

```
default-metric <value>
```

```
no default-metric [<short (1-16)>]
```

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults 3

Example

```
iss(config-router)# default-metric 1
```

☞ The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes.

Related Commands

- **`redistribute`** – Enables redistribution of corresponding protocol routes into RIP
- **`show ip rip`** – Displays IP RIP protocol database or statistics

[1] The metric value given in the no form of the command will be ignored during the execution of the command.

43.11 distance

This command enables the administrative distance (that is, the metric to reach destination) of the routing protocol and sets the administrative distance value. The distance value ranges between 1 and 255.

This distance value will not be used for distribute list. The administrative distance can be enabled for only one route map. The distance should be disabled for the already assigned route map, if distance needs to be enabled for another route map.

The no form of the command disables the administrative distance.

```
distance <1-255> [route-map <name(1-20)>]
```

```
no distance [route-map <name(1-20)>]
```

Syntax Description	**name**	-	Name of the Route Map for which the distance value should be enabled and set. This value is a string of size 20.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults	121		
Example	`iss(config-router)# distance 10 route-map rmap-test`		

☞ RIP should be enabled, before executing this command.

Related Commands

- **`router rip`** – Enables RIP for a specific VRF instance

43.12 auto-summary - enable | disable

This command enables/disables auto summarization of routes in RIP.

auto-summary {enable | disable}

Syntax Description	**enable**	-	Enables auto summarization feature in RIP
	disable	-	Disables auto summarization feature in RIP

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults enable

Example

```
iss(config-router)# auto-summary disable
```

Auto-summarization feature must be disabled to configure interface specific aggregation with RIP version 2.

Related Command

- **show ip rip** – Displays IP RIP protocol database or statistics
- **show ip protocols** - Displays information about the active routing protocol process

43.13 ip rip default route originate

This command sets the metric to be used for default route propagated over the interface. The no form of the command disables origination of default route over the interface.

ip rip default route originate <metric(1-15)>

no ip rip default route originate

Mode	Interface Configuration Mode This command is applicable only in VLAN Interface Mode.
Package	Enterprise and Metro
Defaults	no ip rip default route originate
Example	`iss(config-if)# ip rip default route originate 10`
☞	RIP must be enabled on the interface before executing this command.
Related Commands	• **show ip rip** – Displays IP RIP protocol database or statistics • **show ip protocols** - Displays information about the active routing protocol process • **network** – Enables RIP on an IP network

43.14 ip rip summary-address

This command sets route aggregation over an interface for all subnet routes that falls under the specified IP address and mask. The no form of the command disables route aggregation with the specified IP address and mask.

```
ip rip summary-address <ip-address> <mask>
```

```
no ip rip summary-address <ip-address> <mask>
```

Syntax Description	**ip-address**	-	IP Address of the interface specific aggregation
	mask	-	Subnet Mask
Mode	Interface Configuration Mode This command is applicable only in VLAN Interface Mode.		
Package	Enterprise and Metro		
Example	`iss(config-if)# ip rip summary-address 60.0.0.0 255.0.0.0`		
☞	• This command must not be used with RIPv1 send version. • Auto-summarization overrides interface specific aggregation. Therefore, auto-summarization must be disabled for interface specific route aggregation.		
Related Command	**show ip protocols** - Displays information about the active routing protocol process		

43.15 ip rip default route install

This command installs the default route received in updates to the RIP database. The no form of the command does not install default route received in updates to the rip database.

ip rip default route install

no ip rip default route install

Mode	Interface Configuration Mode This command is applicable only in VLAN Interface Mode.
Package	Enterprise and Metro
Defaults	no ip rip default route install
Example	`iss(config-if)# ip rip default route install`
☞	RIP must be enabled on the interface on which this command is executed.
Related Command	**show ip protocols** - Displays information about the active routing protocol process

43.16 ip rip send version

This command sets the IP RIP version number for transmitting advertisements and the no form of the command sets IP RIP send version number to its default value.

ip rip send version { 1 | 2 | 1 2 | none }

no ip rip send version

Syntax Description	**1 | 2 | 1 2 | none**	- Indicates which version of RIP updates are to be sent. • 1 - Sends RIP updates compliant with RFC 1058. • 2 - Sends multicasting RIP updates. • 1 2 - Sends both multicasting RIP updates and RIP updates compliant with RFC 1058. • none - No RIP updates are send.
Mode	Interface Configuration Mode This command is applicable only in VLAN Interface Mode.	
Package	Enterprise and Metro	
Defaults	1 2	
Example	`iss(config-if)# ip rip send version 1`	
Related Commands	• **ip rip receive version** – Sets IP RIP version number for receiving advertisements • **show ip rip** – Displays IP RIP protocol database or statistics	

43.17 ip rip receive version

This command sets IP RIP version number for receiving advertisements and the no form of the command sets IP RIP receive version number to its default value.

```
ip rip receive version  { 1 | 2 | 1 2 | none }
```

```
no ip rip receive version
```

Syntax Description

`1 | 2 | 1 2 | none`	Indicates which version of RIP updates, are to be accepted. The options are: • 1 - Receives RIP updates compliant with RFC 1058. • 2 - Receives multicasting RIP updates. • 1 2 - Receives both multicasting RIP updates and RIP updates compliant with RFC 1058. • none - No RIP updates are received.

Mode

Interface Configuration Mode

This command is applicable only in VLAN Interface Mode.

Package

Enterprise and Metro

Defaults

1 2

Example

```
iss(config-if)# ip rip receive version 1
```

☞ The command indicates which version of RIP updates are to be accepted. rip2 and rip1 2 implies reception of multicast packets.

Related Commands

- **`ip rip send version`**– Sets IP RIP version number for transmitting advertisements
- **`show ip rip`** – Displays IP RIP protocol database or statistics

43.18 ip rip authentication mode

This command configures authentication mode and key. The no form of the command disables authentication.

```
ip rip authentication mode { text | md5 } key-chain <key-chain-name (16)>
```

```
no ip rip authentication
```

Syntax Description	**text**	-	Clear text authentication.
	md5	-	Keyed Message Digest 5 (MD5) authentication. More than one entry can be configured for an interface.
	key-chain	-	The value to be used as the Authentication Key.

Mode Interface Configuration Mode

This command is applicable only in VLAN Interface Mode.

Package Enterprise and Metro

Defaults No authentication

Example

```
iss(config-if)# ip rip authentication mode text key-chain
asdf123
```

☞ If a string shorter than 16 octets is supplied, it will be left- justified and padded to 16 octets, on the right, with nulls (0x00).

Related Command **show ip rip** – Displays IP RIP protocol database or statistics

43.19 timers basic - update-value

This command sets update, route age and garbage collection timers. The no form of the command sets update, route age and garbage collection timers to the default values.

timers basic <update-value (10-3600)> <routeage-value (30-500)> <garbage-value (120-180)>

no timers basic

Syntax Description	**update-value**	-	Interval Time Between Updates
	routeage-value	-	Time after which the entry is put into garbage collect interval
	garbage-value	-	Interval before deleting an entry after not hearing it
Mode	Interface Configuration Mode This command is applicable only in VLAN Interface Mode.		
Package	Enterprise and Metro		
Defaults	update-value	-	30
	routeage-value	-	180
	garbage-value	-	120

Example

```
iss(config-if)# timers basic 20  40  150
```

☞ The advertisements of garbage-value entry is set to INFINITY, while sending to others.

Related Command

- **show ip rip** – Displays IP RIP protocol database or statistics

43.20 ip split-horizon

This command sets the split horizon status and the no form of the command disables the split horizon status.

ip split-horizon [poisson]

no ip split-horizon

Syntax Description	**poisson**	-	Split horizon with poisson reverse is enabled

Mode Interface Configuration Mode

This command is applicable only in VLAN Interface Mode.

Package Enterprise and Metro

Example

```
iss(config-if)# ip split-horizon
```

☞ The value splitHorizon denotes that splitHorizon must be applied in the response packets that are going out.

Related Command

- **show ip rip** – Displays IP RIP protocol database or statistics

43.21 debug ip rip

This command sets the debug level for RIP module and the no form of the command resets the debug level for RIP module.

debug ip rip [vrf <name>] { all | init | data | control | dump | os | mgmt | failure | buffer }

no debug ip rip [vrf <name>]{ all | init | data | control | dump | os | mgmt | failure | buffer }

Syntax Description	**vrf**	-	Name of the VRF instance. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
	all	-	All resources
	init	-	Initialization and Shutdown messages
	data	-	Data path messages
	control	-	Control Plane messages
	dump	-	Packet Dump messages
	os	-	OS Resource Messages
	mgmt	-	Management messages
	failure	-	All failure messages (All failures including Packet Validation)
	buffer	-	Buffer messages
Mode	Privileged EXEC Mode		
Package	Enterprise and Metro		
Defaults	vrf	-	default
Defaults	init		
Example	`iss# debug ip rip all`		

☞ VRF instance should be created, before executing this command to enable the RIP in the context.

Related Commands

- **ip vrf** - Creates VRF instance
- **show ip rip** – Displays IP RIP protocol database or statistics

43.22 show ip rip

This command displays IP RIP protocol database or statistics.

show ip rip [vrf <name>] { database [<ip-address> <ip-mask>] | statistics }

Syntax Description	**vrf**	-	Name of the VRF instance. This value is a string of size 32.
	database	-	RIP protocol database for the specified IP address and IP mask of the RIP interface entry
	statistics	-	RIP statistics on the router
Mode	Privileged EXEC Mode		
Package	Enterprise and Metro		
Defaults	vrf	-	default

Example

```
iss# sh ip rip vrf default database

Vrf default
12.0.0.0/8   [1]        auto-summary
12.0.0.0/8   [1]        directly connected, vlan1
15.0.0.0/8   [3]        auto-summary
15.0.0.0/8   [3]        directly connected, vlan2
20.0.0.0/8   [4]        auto-summary
20.0.0.0/8   [4]        via 12.0.0.2, vlan1

iss# sh ip rip vrf default statistics

Vrf default

RIP Global Statistics:
----------------------
 Total number of route changes is 1
 Total number of queries responded is 1
 Total number of dropped packets is 0

RIP Interface Statistics:
-------------------------
Interface  Periodic  BadRoutes  Triggered  BadPackets  Admin
IP Address Updates Sent Received Updates Sent Received Status
---------- ----------- -------- ------------ -------- ------
12.0.0.1       19          1         2            0    Enabled
```

Related Commands

- **router rip** – Enables RIP for a specific VRF instance
- **ip rip security** – Accepts/ignores RIP1 packets when authentication is in use
- **ip rip retransmission** – Configures the timeout interval and number of retries

to retransmit the update request packet or an unacknowledged update response packet

- **network** – Enables RIP on an IP network
- **neighbor** – Adds a neighbor router
- **passive-interface vlan** – Suppresses routing updates on an interface
- **output-delay** – Enables interpacket delay for RIP updates
- **redistribute** – Enables redistribution of corresponding protocol routes into RIP
- **default-metric** – Sets the RIP default metric
- **auto-summary enable-disable** - Enables/disables auto summarization of routes in RIP
- **ip rip default route originate** - Sets the metric to be used for default route propagated over the interface
- **ip rip send version** – Sets IP RIP version number for transmitting advertisements
- **ip rip receive version** – Sets IP RIP version number for receiving advertisements
- **ip rip authentication mode** – Configures authentication mode and key
- **timers basic - update- value** – Sets update, route age and garbage collection timers
- **ip split-horizon** – Sets the spilt horizon status
- • **debug ip rip** – Sets the debug level for RIP module

Chapter 44

RIPv6

IPv6 RIP functions the same and offers the same benefits as RIP in IPv4. RIP enhancements for IPv6, detailed in RFC 2080, include support for IPv6 addresses and prefixes, and the use of all-RIP-routers multicast group address as the destination address for RIP update messages. This module describes how to configure Routing Information Protocol for IPv6. IPv6 RIP process maintains a local routing table, referred to as a Routing Information Database (RIB). The IPv6 RIP RIB contains a set of IPv6 RIP routes learnt from all its neighboring networking devices.

Before configuring the router to run IPv6 RIP, the ipv6 unicast-routing must be enabled globally, and IPv6 must be enabled on any interface in which IPv6 RIP is to be processed.

The list of CLI commands for the configuration of RIP6 are as follows:

- ipv6 router rip / ipv6 router rip - name
- ipv6 split-horizon
- ipv6 rip enable / ipv6 rip enable - name
- ipv6 poison reverse
- ipv6 rip default-information originate / ipv6 rip default-information - originate | only
- ipv6 rip metric-offset
- redistribute
- redistribute bgp
- distribute prefix
- distribute-list route-map
- distance
- debug ipv6 rip

- show ipv6 rip
- show ipv6 rip stats
- show ipv6 rip filter

44.1 ipv6 router rip

This command enables RIP6 and enters into the router configuration mode and the no form of the command disables RIP6 on all the interfaces.

ipv6 router rip

no ipv6 router rip

Mode Global Configuration Mode

Package Enterprise and Metro

Example

```
iss(config)# ipv6 router rip
```

☞ Before configuring the router to run IPv6 RIP, the ipv6 unicast-routing must be enabled globally, and IPv6 must be enabled on the interface in which IPv6 RIP is to be processed.

Related Command

- **ipv6 enable** – Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
- **ipv6 unicast-routing** - Enables unicast routing.
- **redistribute** - Enables redistribution of IPv6 prefix from another protocol into RIP6
- **distribute-list route-map** - Enables route map filtering for inbound or outbound routes
- **distance –** Enables the administrative distance of the routing protocol and sets the administrative distance value

44.2 ipv6 router rip - name

This command enables RIP6 and enters into the router configuration mode. The no form of the command disables RIP6 on all the interfaces

This command is a complete standardized implementation of the existing command and operates similar to that of the command ipv6 router rip.

```
ipv6 router rip <name>
```

```
no ipv6 router rip <name>
```

Syntax Description	**name**[2]	-	Specific IPv6 RIP routing process.
Mode	Global Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config)# ipv6 router rip router1`		

☞
- Before configuring the router to run IPv6 RIP, the ipv6 unicast-routing must be enabled globally, and IPv6 must be enabled on the interface in which IPv6 RIP is to be processed.

Related Command
- **ipv6 enable** – Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
- **ipv6 unicast-routing** - Enables unicast routing.

[2] This feature is ignored during the command execution.

44.3 ipv6 split-horizon

This command enables the split horizon updates and the no form of the command disables the split horizon updates.

ipv6 split-horizon

no ipv6 split-horizon

Mode	Interface Configuration Mode
Package	Enterprise and Metro
Example	`iss(config-if)# ipv6 split-horizon`
☞	The value splitHorizon denotes that splitHorizon algorithm must be applied in the response packets that are going out.
Related Command	• **show ipv6 rip** – Displays IPv6 Local RIB and routing protocol information

44.4 ipv6 rip enable

This command enables RIP Routing and the no form of the command disables the RIP Routing.

ipv6 rip enable

no ipv6 rip

Mode	Interface Configuration Mode This command is applicable only in the VLAN interface mode.
Package	Enterprise and Metro
Example	`iss(config-if)# ipv6 rip enable`
Related Command	• **show ipv6 rip** – Displays IPv6 Local RIB and routing protocol information

44.5 ipv6 rip enable - name

This command enables specified IPv6 RIP routing process on an interface. The no form of the command disables the specified routing process on an interface.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ipv6 rip enable.

ipv6 rip <name> enable

no ipv6 rip <name> enable

Syntax Description	**name**[2]	-	Specific IPv6 RIP routing process.
Mode	Interface Configuration Mode This command is applicable only in the VLAN interface mode.		
Package	Enterprise and Metro		
Example	`iss(config-if)# ipv6 rip rip1 enable`		
Related Command	• **show ipv6 rip** – Displays IPv6 Local RIB and routing protocol information		

44.6 ipv6 poison reverse

This command enables poison reverse.

`ipv6 poison reverse`

Mode	Interface Configuration Mode
Package	Enterprise and Metro
Example	`iss(config-if)# ipv6 poison reverse`
☞	The value poison reverse denotes that poison reverse algorithm must be applied in the response packets that are going out.
Related Command	• **`show ipv6 rip`** – Displays IPv6 Local RIB and routing protocol information

44.7 ipv6 rip default-information originate

This command configures handling of default route originate. This command originates the IPv6 default route into the specified RIP routing process updates sent out of the specified interface. The no form of the command disables handling of default route originate.

ipv6 rip default-information originate

no ipv6 rip default-information

Mode	Interface Configuration Mode This command is applicable only in the VLAN interface mode.
Package	Enterprise and Metro
Example	`iss(config-if)# ipv6 rip default-information originate`
Related Command	• **show ipv6 rip** – Displays IPv6 Local RIB and routing protocol information

44.8 ipv6 rip default-information - originate | only

This command originates the IPv6 default route into the specified RIP routing process updates, sent from the specified interface.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ipv6 rip default-information originate.

The routing process ignores all default routes received on any interface, after originating the IPv6 default route out of any interface to avoid routing loops.

`ipv6 rip <process-name> default-information { originate | only } [metric <value>]`

Syntax Description	**`process-name`**[2]	- Specific IPv6 RIP routing process.
	`originate`	- Default route is originated in addition to all other routes in the updates sent from the interface.
	`only`	- Default route is originated while suppressing all other routes in the updates sent from the interface. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
	`metric`	- Metric to be used for redistributed routes. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
Mode	Interface Configuration Mode This command is applicable only in the VLAN interface mode.	
Package	Enterprise and Metro	
Example	`iss(config-if)# ipv6 rip process1 default-information originate`	
Related Command	• **`show ipv6 rip`** – Displays IPv6 Local RIB and routing protocol information	

44.9 ipv6 rip metric-offset

This command adjusts default metric increment.

ipv6 rip metric-offset <integer (1-15)>

Mode	Interface Configuration Mode
Package	Enterprise and Metro
Example	`iss(config-if)# ipv6 rip metric-offset 6`

☞

- The ipv6 rip metric-offset command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes.
- The maximum metric that RIP can advertise is 16, and a metric of 16 denotes a route that is unreachable.

Related Command

- **show ipv6 rip** – Displays IPv6 Local RIB and routing protocol information

44.10 redistribute

This command enables redistribution of IPv6 prefix from another protocol into RIP6. The redistribution is done after applying the route map, if the route map is specified. The no form of the command disables redistribution of IPv6 prefix from another protocol into RIP6. The route map is disassociated for redistribution, if the no form of the command specifies the route map.

```
redistribute {static|connected|ospf} metric <integer(0-16)> [route-map
<string(20)>]
```

```
no redistribute {static|connected|ospf} [route-map <string(20)>]
```

Syntax Description	**static**	-	Statically configured routes to advertise in the RIP6 process
	connected	-	Connected routes to advertise in the RIP6 process
	ospf	-	OSPF routes to advertise in the RIP6 process
	metric	-	Routing metric associated with the route
	route-map	-	Name of the Route Map to be applied during redistribution of routes to RIPv6. If this is not specified, all routes are redistributed. This value is a string of size 20.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# redistribute static metric 6`		
☞	RIP6 should enabled, before executing this command		

Related Command

- **ipv6 router rip** - Enables RIP6
- **show ipv6 rip** – Displays IPv6 Local RIB and routing protocol information

44.11 redistribute bgp

This command redistributes IPv6 prefix from another protocol into RIP6.

This command has been included to adhere to the Industry Standard CLI syntax. This command is currently not supported.

```
redistribute bgp <as-no> [metric <integer(0-16)>]
```

Syntax Description	**as-no**	-	Autonomous number of the router. This value ranges between 1 and 65535.
	metric	-	Metric to be used for redistributed routes. This value ranges between 0 and 16.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# redistribute bgp 10 metric 10`		

☞
- A route must be advertised with a metric of value 15 or less, as the RIP router always adds an interface cost (default 1) onto the metric of the received route. This makes the metric 16, which denotes that the route is unreachable.

44.12 distribute prefix

This command enables Filter network in routing updates sent or received and the no form of the command disables Filter network in routing updates sent or received.

distribute prefix <ip6_addr> {in | out}

no distribute prefix <ip6_addr> {in | out}

Syntax Description	**ip6_addr**	-	IPv6 Address
	in	-	Filter network in routing updates received
	out	-	Filter network in routing updates sent out
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# distribute prefix fe80::208:2ff:fe02:408 in`		

☞

- Filtering is controlled by distribute lists. Input distribute lists control route reception and input filtering is applied to advertisements received from neighbors. Only those routes that pass input filtering are inserted in the RIP local routing table and become candidates for insertion into the IPv6 routing table.
- Output distribute lists control route advertisement. Output filtering is applied to route advertisements sent to neighbors. Only those routes passing output filtering will be advertised.

Related Commands

- **show ipv6 rip** – Displays IPv6 Local RIB and routing protocol information
- **show ipv6 rip filter** – Displays peer and Advfilter table

44.13 distribute-list route-map

This command enables route map filtering for inbound or outbound routes. The no form of the command disables route map filtering for inbound or outbound routes

distribute-list route-map <name(1-20)> {in | out}

no distribute-list route-map <name(1-20)> {in | out}

Syntax Description	**name**	-	Name of the Route Map for which filtering should be enabled. This value is a string of size 20.
	in	-	Filtering is set for inbound routes.
	out	-	Filtering is set for outbound routes.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# distribute-list route-map rmap-test in`		
☞	RIP6 should enabled, before executing this command		
Related Command	• **ipv6 router rip** - Enables RIP6 • **show running-config rip6** - Displays the current operating configuration in the syste		

44.14 distance

This command enables the administrative distance (that is, the metric to reach destination) of the routing protocol and sets the administrative distance value. The distance value ranges between 1 and 255.

The no form of the command disables the administrative distance.

```
distance <1-255> [route-map <name(1-20)>]
```

```
no distance [route-map <name(1-20)>]
```

Syntax Description	**name**	-	Name of the Route Map for which the distance value should be enabled and set. This value is a string of size 20.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults	120 (Represents RIP route)		
Example	`iss(config-router)# distance 10 route-map rmap-test`		
☞	RIP6 should enabled, before executing this command		
Related Command	• **ipv6 router rip** - Enables RIP6 • **show running-config rip6** - Displays the current operating configuration in the system		

44.15 debug ipv6 rip

This command enables IPv6 RIP routing protocol debugging and the no form of the command disables IPv6 RIP routing protocol debugging.

debug ipv6 rip { all | data | control }

no debug ipv6 rip

Syntax Description	**all**	-	All resources
	data	-	Data path messages
	control	-	Control Plane messages
Mode	Privileged EXEC Mode		
Package	Enterprise and Metro		
Defaults	Disabled		
Example	`iss# debug ipv6 rip all`		
Related Command	• **show ipv6 rip** – Displays IPv6 Local RIB and routing protocol information		

44.16 show ipv6 rip

This command displays IPv6 Local RIB and routing protocol information.

show ipv6 rip [database]

Syntax Description	**database**	-	IPv6 RIP protocol database

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ipv6 rip database

RIP local RIB
4444::/64,  metric 10, local
      vlan1/::, expires in 180 secs
5555::/64,  metric 10, local
      vlan2/::, expires in 180 secs
6666::/64,  metric 7, static
      tunnel0/::, expires in 180 secs
```

Related Commands

- **ipv6 router rip** – Enables the router configuration mode
- **ipv6 split-horizon** – Enables the split horizon updates
- **ipv6 rip enable / ipv6 rip enable – name** – Enables RIP Routing
- **ipv6 poison reverse** – Enables poison reverse
- **ipv6 rip default-information originate** – Configures handling of default route originate
- **ipv6 rip default-information – originate | only**- Originates the IPv6 default route into the specified RIP routing process updates sent from the specified interface.
- **ipv6 rip metric-offset** – Adjusts default metric increment
- **redistribute** – Redistributes IPv6 prefix from another protocol into RIP6
- **distribute prefix** – Enables Filter network in routing updates sent or received
- **debug ipv6 rip** – Enables IPv6 RIP routing protocol debugging

44.17 show ipv6 rip stats

This command displays all the interface statistics.

show ipv6 rip stats

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ipv6 rip stats

        Interface Index     vlan1
        *****************    ***
Rcvd  :
Messages          0    Requests       0   Responses       0
UnknownCommds     0    OtherVer       0   Discards        0
Sent  :
Messages          1    Requests       1   Responses       0
Trigger Updates   0
```

44.18 show ipv6 rip filter

This command displays peer and Advfilter table.

show ipv6 rip filter

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ipv6 rip filter

Filter Address                    FilterType
**************                    **********

fe80::200:ff:febb:e01                    IN
fe80::200:ff:fecc:102                    IN
3333::1111                               OUT
```

Related Command

- **distribute prefix** – Enables Filter network in routing updates sent or received

Chapter 45

BGP

The BGP (Border Gateway Protocol) is an inter-autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems and is used between Internet service providers (ISP). BGP is often the protocol used between gateway hosts on the Internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen.

Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when one host has detected a change. BGP is commonly used within and between Internet Service Providers (ISPs). The protocol is defined in RFC 1771.

The list of CLI commands for the configuration of BGP is as follows:

- router bgp
- ip bgp dampening / bgp dampening
- ip bgp overlap-policy
- default-information originate
- ip bgp synchronization / synchronization
- bgp router-id
- bgp default local-preference
- bgp default ipv4-unicast
- neighbor - remote-as

- neighbor - activate
- neighbor - ebgp-multihop
- neighbor - next-hop-self
- neighbor - interval
- neighbor - timers
- neighbor - shutdown
- neighbor - update-source
- neighbor – gateway
- neighbor - network-address
- neighbor - default-originate
- neighbor - send-community
- neighbor - capability
- bgp nonbgproute-advt
- redistribute
- import route
- bgp always-compare-med
- default-metric
- bgp med
- bgp local-preference
- bgp update-filter
- aggregate-address index
- bgp cluster-id
- bgp client-to-client reflection
- neighbor - route-reflector-client
- bgp comm-route
- bgp comm-filter
- bgp comm-policy
- bgp ecomm-route
- bgp ecomm-filter
- bgp ecomm-policy
- bgp confederation identifier
- bgp confederation peers
- bgp bestpath med confed
- neighbor - password
- import ipv6-route

- address-family
- clear ip bgp
- clear bgp ipv6
- shutdown ip bgp
- debug ip bgp
- show bgp-version
- show ip bgp
- show ip bgp community - routes
- show ip bgp extcommunity - routes
- show ip bgp summary
- show ip bgp filters
- show ip bgp aggregate
- show ip bgp med
- show ip bgp dampening
- show ip bgp local-pref
- show ip bgp timers
- show ip bgp info
- show ip bgp rfl info
- show ip bgp confed info
- show ip bgp community
- show ip bgp extcommunity
- show bgp ipv6

45.1 router bgp

This command sets the AS number of the BGP Speaker. The no form of the command brings the BGP Speaker Global Admin status DOWN and resets the AS number of the BGP Speaker.

```
router bgp <AS no(1-65535)>
```

```
no router bgp
```

Syntax Description	**AS no**	-	Autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 1 and 65535.
Mode	Global Configuration Mode		
Package	Enterprise and Metro		
Defaults	0		
Example	`iss(config)# router bgp 100`		

☞
- The command makes the BGP speaker Global Admin Status ACTIVE.
- The autonomous number and the router ID must be set for the router before setting the AS number for the BGP speaker.

Related Commands

- **as-num** - Sets the autonomous number for the router.
- **router-id** - Sets the router ID's address for the router.
- **ip bgp dampening** – Configures the Dampening Parameters
- **ip bgp overlap-policy** – Configures the Overlap Route policy for the BGP Speaker
- **ip bgp synchronization / synchronization** – Enables synchronization between BGP and IGP
- **bgp router-id** – Configures the BGP Identifier of the BGP Speaker
- **bgp default local-preference** – Configures the Default Local Preference value
- **neighbor – remote-as** – Creates a Peer and initiates the connection to the peer
- **neighbor – activate** - Resets configured network-address for peer
- **neighbor – ebgp-multihop** – Enables BGP to establish connection with external peers
- **neighbor – next-hop-self** – Enables BGP to send itself as the next hop for advertised routes
- **neighbor – interval** – Configures neighbor interval
- **neighbor – timers**– Configures neighbor KeepAlive Time and Hold Time Intervals
- **neighbor – shutdown** – Disables the Peer session
- **neighbor – update-source** - Configures the source-address for routing updates and for TCP connection establishment with a peer
- **neighbor – gateway** - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer
- **neighbor – network-address** - Configures peer's remote IPv6 network address for IPv4 peer and peer's remote IPv4 network address for IPv6 peer
- **neighbor – default – originate** - Enables advertisement of the default route to the peer
- **neighbor – send-community** – Enables advertisement of community attributes to (standard/extended) to peer
- **neighbor – capability** - Enables the specific BGP capability to be advertised and received from the peer
- **bgp nonbgproute-advt** – Controls the advertisement of Non-BGP routes
- **no ip bgp overlap-policy** – Resets the Overlap route policy to default
- **redistribute** – Configures the protocol from which the routes have to be redistributed into BGP
- **bgp always-compare-med** – Enables the comparison of med for routes received from different autonomous system
- **default-metric** – Configures the Default IGP Metric value
- **bgp med** – Configures an entry in MED Table
- **bgp local-preference** – Configures an entry in Local Preference Table
- **bgp update-filter** – Configures an entry in Update Filter Table
- **aggregate-address index** – Configures an entry in Aggregate Table

45.2 ip bgp dampening

This command configures the Dampening parameters and the no form of the command resets the Dampening parameters to default.

```
ip bgp dampening [HalfLife-Time <integer(600-2700)>] [Reuse-Value <integer(15-10800)>] [Suppress-Value <integer(2000-3999)>] [Max-Suppress-Time <integer(1800-10800)>] [-s Decay-Granularity <integer(1-10800)>] [Reuse-Granularity <integer(15-10800)>] [Reuse-Array-Size <integer(256-65535)>]
```

```
no ip bgp dampening [HalfLife-Time [Reuse-Value [Suppress-Value [Max-Suppress-Time]]]] [-s [Decay-Granularity [Reuse-Granularity [Reuse-Array-Size]]]
```

Syntax Description

HalfLife-Time	-	Time (in seconds) after which a penalty is decreased by half. Once a route has been assigned a penalty, the penalty is decreased for every 5 seconds. This value ranges between 600 and 2700.
Reuse Value	-	If the penalty associated with a suppressed route falls below this value, the route is re-used. This value ranges between 15 and 10800.
Suppress Value	-	A route is suppressed when the penalty associated with the route exceeds this value. This value ranges between 2000 and 3999.
Max-Suppress Time	-	Maximum time (in seconds) a route can be suppressed. This value ranges between 1800 and 10800.
Decay Granularity	-	Time granularity in seconds used to perform all decay computations. This value ranges between 1 and 10800.
Reuse Granularity	-	Time interval between evaluations of the reuse-lists. Each reuse lists corresponds to an additional time increment. This value ranges between 15 and 10800.
Reuse Array Size	-	Size of reuse index arrays. This size determines the accuracy with which suppressed routes can be placed within the set of reuse lists when suppressed for a long time. This value ranges between 256 and 65535.

Mode	Global Configuration Mode		
Package	Enterprise and Metro		
Defaults	HalfLife-Time	-	900
	Reuse Value	-	500
	Suppress Value	-	3500
	Max-Suppress Time	-	3600
	Decay Granularity	-	1
	Reuse Granularity	-	15
	Reuse Array Size	-	1024

Example

```
iss(config)# ip bgp dampening 1000
```

☞

Related Commands

- BGP Speaker Local AS number must be configured
- BGP Administrative status must be DOWN (use Shutdown Command)
- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`shutdown ip bgp`** – Sets the BGP Speaker Global Admin status DOWN
- **`show ip bgp dampening`** – Displays the contents of dampening table

45.3 bgp dampening

This command configures the Dampening Parameters and the no form of the command resets the Dampening Parameters to default.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip bgp dampening.

bgp dampening [HalfLife-Time <integer(600-2700)>] [Reuse-Value <integer(15-10800)>] [Suppress-Value <integer(2000-3999)>] [Max-Suppress-Time <integer(1800-10800)>]

no bgp dampening

Syntax Description

HalfLife-Time	-	Time (in seconds) after which a penalty is decreased by half. Once a route has been assigned a penalty, the penalty is decreased for every 5 seconds. This value ranges between 600 and 2700. BGP's route flap damping algorithm calculates penalty for each routes. This penalty increases by a fixed value when a flap occurs, and decreases exponentially when the route is stable.
Reuse Value	-	If the penalty associated with a suppressed route falls below this value, the route is re-used. This value ranges between 15 and 10800.
Suppress Value	-	A route is suppressed when the penalty associated with the route exceeds this value. This value ranges between 2000 and 3999.
Max-Suppress Time	-	Maximum time (in seconds) a route can be suppressed. This value ranges between 1800 and 10800.

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults

HalfLife-Time	-	900
Reuse Value	-	500
Suppress Value	-	3500
Max-Suppress Time	-	3600

Example

```
iss(config-router)# bgp dampening 1000
```

- BGP Speaker Local AS number must be configured
- BGP Administrative status must be DOWN (use Shutdown Command)

- Reuse value cannot be configured without configuring the HalfLife Time.
- Suppress value cannot be configured without configuring the HalfLife Time and Reuse value.
- Max-Suppress Time cannot be configured without configuring the HalfLife Time, Reuse Value and Suppress Value.

Related Commands

- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`shutdown ip bgp`** – Sets the BGP Speaker Global Admin status DOWN
- **`show ip bgp dampening`** – Displays the contents of dampening table

45.4 ip bgp overlap-policy

This command configures the Overlap Route policy for the BGP Speaker. The no form of the command Resets the Overlap route policy to default. By default, both less and more specific routes are installed.

ip bgp overlap-policy <more-specific|less-specific|both>

no ip bgp overlap-policy

Syntax Description	**more-specific**	-	This installs only more-specific routes in the RIB
	less-specific	-	This installs only less-specific routes in the RIB
	both	-	This installs all routes(more-specific and less-specific) in the RIB

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults Both

Example

```
iss(config)# ip bgp overlap-policy more-specific
```

☞ **Related Commands**

- BGP Speaker Local AS number must be configured
- BGP Speaker Admin Status must be DOWN
- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp info** – Displays the general info about BGP protocol
- **shutdown ip bgp** – Sets the BGP Speaker Global Admin status DOWN
- **show ip bgp summary** – Displays the status of all BGP4 connections

45.5 default-information originate

This command enables redistribution and advertisement of the default route (0.0.0.0/0). The no form of the command disables redistribution and advertisement of the default route.

default-information originate

no default-information originate

Mode	Global Configuration Mode
Package	Enterprise and Metro
Defaults	The **Default Originate** is disabled (that is, the default routes are not redistributed into BGP).
Example	`iss(config)# default-information originate`
☞	• The default route advertisement is possible only if the default route is present in the IP FDB or it is received from any peers • This command can be executed only if the local AS number is set for the BGP speaker.
Related Commands	• **router bgp** – Sets the AS number of the BGP Speaker. • **show ip bgp info** - Displays the general information about BGP protocol. • **show running-config bgp** - Displays the current operating configuration in the system.

45.6 ip bgp synchronization

This command enables synchronization between BGP and IGP and the no form of the command disables synchronization between BGP and IGP.

`ip bgp synchronization`

`no ip bgp synchronization`

Mode	Global Configuration Mode
Package	Enterprise and Metro
Defaults	Disable
Example	`iss(config)# ip bgp synchronization`

☞

Related Commands

- BGP Speaker Local AS number must be configured
- BGP must be administratively down
- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`show ip bgp info`** – Displays the general info about BGP protocol
- **`shutdown ip bgp`** – Sets the BGP Speaker Global Admin status DOWN

45.7 synchronization

This command enables synchronization between BGP and IGP and the no form of the command disables synchronization between BGP and IGP.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip bgp synchronization.

synchronization

no synchronization

Mode	Router Configuration Mode
Package	Enterprise and Metro
Defaults	The synchronization between the BGP and IGP is disabled.
Example	`iss(config-router)# synchronization`
☞ **Related Commands**	• BGP Speaker Local AS number must be configured • BGP must be administratively down • **router bgp** – Sets the AS number of the BGP Speaker • **show ip bgp info** – Displays the general info about BGP protocol • **shutdown ip bgp** – Sets the BGP Speaker Global Admin status DOWN

45.8 bgp router-id

This command configures the BGP Identifier of the BGP Speaker and the no form of the command resets the BGP Identifier of the BGP Speaker to default value.

bgp router-id <bgp router id (ip-address)>

no bgp router-id

Mode	Router Configuration Mode
Package	Enterprise and Metro
Defaults	The highest interface address is used as the router id
Example	`iss(config-router)# bgp router-id 10.0.0.1`

☞

- BGP router id is a unique number associated with the BGP speaker. This router-id is advertised to other peers and identifies the BGP speaker uniquely
- Administrator can set the router-id of BGP to any value. If router-id is changed, then all the active peer sessions will go DOWN and will be re-started with the new configured router-id
- BGP Speaker Local AS number must be configured

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp** – Displays the BGP related information
- **show ip bgp summary** – Displays the status of all BGP4 connections

45.9 bgp default local-preference

This command configures the Default Local Preference value and the no form of the command resets the Default Local Preference to its default value.

bgp default local-preference <Local Pref Value>

no bgp default local-preference

Mode	Router Configuration Mode
Package	Enterprise and Metro
Defaults	100
Example	`iss(config-router)# bgp default local-preference 100`

☞
- BGP Speaker Local AS number must be configured
- If required administrator can use this command to change this Default Local Preference value

Related Commands
- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp info** – Displays the general info about BGP protocol
- **show ip bgp summary** – Displays the status of all BGP4 connections

45.10 bgp default ipv4-unicast

This command sets default routing to IPv4-unicast. The no form of the command resets the default routing configuration.

The MP IPv4 Unicast Address Family Capability will be negotiated for a peer, if the neighbor is created and the default routing is set to IPv4-unicast. It will not be negotiated for a peer if the default routing configuration is reset.

This command affects the negotiation of the MP IPv4 Unicast Address Family Capability and will not affect the MP IPV4 Unicast negotiation status of the already existing peer.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Mode	Router Configuration Mode
Package	Enterprise and Metro
Defaults	The default routing is set as IPv4-unicast.
Example	`iss(config-router)# bgp default ipv4-unicast`
☞	• This command can be executed only if the local AS number is set for the BGP speaker.
Related Commands	• **router bgp** – Sets the AS number of the BGP Speaker. • **show running-config bgp** - Displays the current operating configuration in the system.

45.11 neighbor - remote-as

This command creates a Peer and initiates the connection to the peer and the no form of the command disables the peer session and deletes the peer information.

neighbor <ip-address | peer-group-name> remote-as <AS no(1-65535)>

no neighbor <ip-address | peer-group-name> [remote-as <AS no(1-65535)>]

Syntax Description	**ip-address**	- BGP peer's remote IP address.
	peer-group-name	- Name of a BGP peer group.
	remote-as	- Autonomous system to which the BGP peer belongs. This value ranges between 1 and 65535. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# neighbor 23.45.0.1 remote-as 200
```

☞

- BGP Speaker Local AS number must be configured
- The administrator can create a peer and set the peer AS number with this command. This configured peer AS number is compared with the AS number received in the open message and a peer session is initiated only if both the AS numbers match

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor – activate** - Resets configured network-address for peer
- **neighbor – ebgp-multihop** – Enables BGP to establish connection with external peers
- **neighbor – next-hop-self** – Enables BGP to send itself as the next hop for advertised routes
- **neighbor – interval** – Configures neighbor interval
- **neighbor – timers**– Configures neighbor KeepAlive Time and Hold Time Intervals
- **neighbor – shutdown** – Disables the Peer session

- **neighbor – update-source** - Configures the source-address for routing updates and for TCP connection establishment with a peer
- **neighbor – gateway** - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer
- **neighbor – network-address** - Configures peer's remote IPv6 network address for IPv4 peer and peer's remote IPv4 network address for IPv6 peer
- **neighbor – default-originate** - Enables advertisement of the default route to the peer
- **neighbor – send-community** – Enables advertisement of community attributes to (standard/extended) to peer
- **neighbor – capability** - Enables the specific BGP capability to be advertised and received from the peer
- **neighbor – password** – Configures the password for TCP-MD5 authentication with peer
- **show ip bgp summary** – Displays the status of all BGP4 connections
- **show ip bgp** – Displays the BGP related information
- **show ip bgp restart mode** - Displays the restart mode of the BGP router and neighbors
- **show ip bgp EndOfRIBMarkerStatus** - Displays the End_Of_RIB marker status of the BGP router and neighbors
- **show ip bgp restartexitreason** - Displays the restart exit reason of the BGP
- **show ip bgp restartsupport** - Displays the restart support of the BGP
- **show ip bgp restartstatus** - Displays the restart status of the BGP
- **show ip bgp timers** - Displays the value of BGP timers
- **show ip bgp info** – Displays the general info about BGP protocol
- **show running-config bgp** - Displays the current operating configuration in the system.
- **show bgp ipv6** - Displays the BGPv6 related information

45.12 neighbor - activate

This command resets configured network-address for peer. The no form of the command resets the peer after disabling the default capabilities associated with the address-family mode.

neighbor <ip-address> activate

no neighbor <ip-address> activate

Syntax Description	**ip-address**	-	BGP peer's IP address
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults			
Example	`iss(config-router)# neighbor 23.45.0.1 activate`		

☞
- BGP Speaker Local AS number must be configured
- Peer must have been created and peer AS must be configured

Related Commands
- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **show running-config bgp** - Displays the current operating configuration in the system

45.13 neighbor - ebgp-multihop

This command enables BGP to establish connection with external peers that are not directly connected and the no form of the command resets the peer EBGP-Multihop status to default.

neighbor <ip-address | peer-group-name> ebgp-multihop

no neighbor <ip-address | peer-group-name> ebgp-multihop

Syntax Description	**ip-address**	- Peer's IP address
	peer-group-name	- Name of a BGP peer group This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults EBGP Multihop is disabled.

Example

```
iss(config-router)# neighbor 23.45.0.1 ebgp-multihop
```

☞

- By default external BGP peers need to be directly connected. If external BGP peer are not connected directly, then ebgp-multihop is enabled to initiate the connection with that external peer. If ebgp-multihop is disabled and external BGP peers are indirectly connection, then BGP peer session will not be established
- BGP Speaker Local AS number must be configured
- Peer must have been created and peer AS must be configured

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **show ip bgp info** – Displays the general info about BGP protocol
- **show running-config bgp** - Displays the current operating configuration in the system
- **show bgp ipv6** - Displays the BGPv6 related information

45.14 neighbor - next-hop-self

This command enables BGP to send itself as the next hop for advertised routes and the no form of the command resets the peer nexthop-self status to default. By default, Self Next Hop is disabled.

neighbor <ip-address | peer-group-name> next-hop-self

no neighbor <ip-address | peer-group-name> next-hop-self

Syntax Description	**ip-address**	- The IP address of the BGP peer
	peer-group-name	- Name of a BGP peer group. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults The next hop will be generated based on the IP address of the destination and the present next hop in the route information.

Example

```
iss(config-router)# neighbor 23.45.0.1 next-hop-self
```

☞

- Administrator can use this command to make BGP speaker fill its address when advertising routes to the BGP peer
- BGP Speaker Local AS number must be configured
- Peer must have been created and peer AS must be configured

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor – remote-as** – Creates a Peer and initiates the connection to the peer
- **show ip bgp info** – Displays the general info about BGP protocol
- **show bgp ipv6** - Displays the BGPv6 related information
- **show running-config bgp** - Displays the current operating configuration in the system

45.15 neighbor - interval

This command configures neighbor interval and the no form of the command resets neighbor interval.

```
neighbor <ip-address | peer-group-name> {advertisement-interval <seconds(1-65535)> | as-origination-interval <seconds(1-65535)> | connect-retry-interval <seconds(1-65535)>}
```

```
no neighbor <ip-address | peer-group-name> {advertisement-interval | as-origination-interval | connect-retry-interval}
```

Syntax Description

ip-address	-	BGP peer's IP address
peer-group-name	-	Name of a BGP peer group. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
advertisement-interval	-	The time-interval (in seconds) for spacing advertisement of successive external route-updates to the same destination. This value ranges between 1 and 65535.
as-origination-interval	-	The time-interval (in seconds) for spacing successive route-updates originating within the same AS. This value ranges between 1 and 65535.
connect-retry-interval	-	The time interval (in seconds) after which a transport connection with peer is re-initiated. This value ranges between 1 and 65535.

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults

advertisement-interval	-	30 seconds
as-origination-interval	-	15 seconds
connect-retry-interval	-	30 seconds

Example

```
iss(config-router)# neighbor 23.45.0.1 advertisement-interval 45
```

☞
- BGP Speaker Local AS number must be configured
- Peer must have been created and peer AS must be configured

Related Commands

- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`neighbor - remote-as`** – Creates a Peer and initiates the connection to the peer
- **`show ip bgp info`** – Displays the general info about BGP protocol
- **`show ip bgp timers`** - Displays the value of BGP timers
- **`show running-config bgp`** - Displays the current operating configuration in the system
- **`show bgp ipv6`** - Displays the BGPv6 related information

45.16 neighbor - timers

This command configures neighbor KeepAlive Time and Hold Time Intervals and the no form of the command resets neighbor KeepAlive Time and Hold Time Intervals.

```
neighbor <ip-address | peer-group-name> timers {keepalive < (1-21845) seconds>
| holdtime < (3-65535) seconds>}
```

```
no neighbor <ip-address | peer-group-name> timers {keepalive | holdtime}
```

Syntax Description

ip-address	-	BGP peer's IP address
peer-group-name	-	Name of a BGP peer group. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
timers	-	Timer value • **keepalive** - Keep-alive interval (in seconds) for the peer session.The keep-alive value must always be less than the configured hold-time value. • **holdtime –** The hold-time interval (in seconds) for the peer. This is sent in the OPEN message to the peer. The system declares a peer dead, after not receiving a keepalive message within this time period from the peer.

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults

keepalive	-	30 seconds
holdtime	-	90 seconds

Example

```
iss(config-router)# neighbor 23.45.0.1 timers keepalive 40
```

☞
- BGP Speaker Local AS number must be configured
- Peer must be created and peer AS must be configured

Related Commands

- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`neighbor - remote-as`** – Creates a Peer and initiates the connection to the peer
- **`show ip bgp info`** – Displays the general info about BGP protocol
- **`show ip bgp timers`** - Displays the value of BGP timers
- **`show running-config bgp`** - Displays the current operating configuration in the system
- **`show bgp ipv6`** - Displays the BGPv6 related information

45.17 neighbor - shutdown

This command disables the Peer session and the no form of the command enables the Peer session.

```
neighbor <ip-address | peer-group-name> shutdown
```

```
no neighbor <ip-address | peer-group-name> shutdown
```

Syntax Description

ip-address	-	BGP peer's IP address
peer-group-name	-	Name of a BGP peer group. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
shutdown	-	Terminates the peer session

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# neighbor 23.45.0.1 shutdown
```

☞

- BGP Speaker Local AS number must be configured
- Peer must be created and peer AS must be configured

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **show ip bgp** – Displays the BGP related information
- **show running-config bgp** - Displays the current operating configuration in the system
- **show bgp ipv6** - Displays the BGPv6 related information

45.18 neighbor - update-source

This command configures the source-address for routing updates and for TCP connection establishment with a peer. The no form of the command disables configured source-address for routing updates and for TCP connection establishment with a peer.

neighbor <ip-address> update-source <random_str>

no neighbor <ip-address> update-source <random_str>

Syntax Description	**ip-address**	- BGP peer's IP address
	random_str	- IP address to be used as source for routing updates and TCP connection establishment. This IP address can be any interface address.
Mode	Router Configuration Mode	
Package	Enterprise and Metro	
Defaults	The source address is set as 0.0.0.0, and the TCP fills the source address of the TCP session.	
Example	`iss(config-router)# neighbor 23.45.0.1 update-source 40.0.0.1`	

☞

Related Commands

- BGP Speaker Local AS number must be configured
- Peer must have been created and peer AS must be configured
- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **show running-config bgp** - Displays the current operating configuration in the system.
- **show ip bgp** – Displays the BGP related information
- **show bgp ipv6** - Displays the BGPv6 related information

45.19 neighbor – gateway

This command configures gateway router's address that will be used as nexthop in the routes advertised to the peer. The no form of the command resets the configured gateway router's address.

neighbor <ip-address> gateway <random_str>

no neighbor <ip-address> gateway <random_str>

Syntax Description	**ip-address**	-	BGP peer's IP address
	random_str	-	IP address of the gateway to be used as next hop
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# neighbor 23.45.0.1 gateway 10.0.0.1`		

☞

Related Commands

- BGP Speaker Local AS number must be configured
- Peer must have been created and peer AS must be configured
- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **show running-config bgp** - Displays the current operating configuration in the system.
- **show ip bgp** – Displays the BGP related information
- **show bgp ipv6** - Displays the BGPv6 related information

45.20 neighbor - network-address

This command configures peer's remote IPv6 network address for IPv4 peer and peer's remote IPv4 network address for IPv6 peer. The no form of the command resets network-address configured for the peer.

The peer's network address carries the IPv6 network address if the peer's remote-address is an IPv4 address. The peer's network address carries the IPv4 network address if the peer's remote-address is an IPv6 address.

```
neighbor <ip-address> network-address <random_str>
```

```
no neighbor <ip-address> network-address <random_str>
```

Syntax Description	**ip-address**	-	BGP peer's IP address
	random_str	-	Remote IP address of the peer

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# neighbor 23.45.0.1 network-address 3399::11

iss(config-router)# neighbor 3399::11 network-address 23.45.0.1
```

☞

- BGP Speaker Local AS number must be configured
- Peer must have been created and peer AS must be configured
- The peer's remote network address can be configured only after configuring the peer's remote address and the corresponding local interface.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **show running-config bgp** - Displays the current operating configuration in the system

45.21 neighbor - default-originate

This command enables advertisement of the default route to the peer. The no form of the command disables advertisement of the default route to the peer.

neighbor <ip-address|peer-group-name> default-originate

no neighbor <ip-address|peer-group-name> default-originate

Syntax Description

ip-address	-	BGP peer's IP address
peer-group-name	-	Name of a BGP peer group. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults The advertisement of default route to the peer is disabled.

Example

```
iss(config-router)# neighbor 23.45.0.1 default-originate
```

☞

- BGP Speaker Local AS number must be configured
- Peer must have been created and peer AS must be configured
- This command overrides the global default route configuration and sends a default route to the peer with self next-hop.
- The advertisement occurs irrespective of the presence of default route in FDB.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **show running-config bgp** - Displays the current operating configuration in the system

45.22 neighbor - send-community

This command enables advertisement of community attributes to (standard/extended) peer and the no form of the command disables advertisement of community attributes to (standard/extended) peer.

neighbor <ip-address> send-community {both | standard | extended}

no neighbor <ip-address> send-community {both | standard |extended}

Syntax Description

ip-address	- Peer IP address
send-community	- Sends Communities. • **both** - Send both communities and extended communities to peer • **standard -** Send only communities to the peer • **extended** - Send only extended communities to peer

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults both

Example

```
iss(config-router)# neighbor 23.45.0.1 send-community both
```

☞

Related Commands

- Peer must be created and peer AS must be configured
- BGP Speaker Local AS number must be configured
- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **show ip bgp community** – Displays the contents of community route/peer/policy/ filter tables
- **show running-config bgp** - Displays the current operating configuration in the system

45.23 neighbor - capability

This command enables the specific BGP capability to be advertised and received from the peer. The no form of the command disables the capability for the peer.

neighbor <ip-address|peer-group-name> capability <ipv4-unicast|ipv6-unicast| route-refresh>

no neighbor <ip-address|peer-group-name> capability <ipv4-unicast|ipv6-unicast| route-refresh>

Syntax Description

ip-address	-	BGP peer's IP address
peer-group-name	-	Name of a BGP peer group. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
ipv4-unicast	-	MP IPv4 unicast address family capability
ipv6-unicast	-	MP IPv6 unicast address family capability
route-refresh	-	Route refresh capability

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# neighbor 23.45.0.1 capability ipv4-unicast
```

☞

- BGP Speaker Local AS number must be configured
- Peer must have been created and peer AS must be configured
- The IPv4 unicast address family capability can be set only for the IPv4 peer.
- The IPv6 unicast address family capability can be set only for the IPv6 peer.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor – remote-as** – Creates a Peer and initiates the connection to the peer
- **show running-config bgp** - Displays the current operating configuration in the system

45.24 bgp nonbgproute-advt

This command controls the advertisement of Non-BGP routes either to the external peer or both to internal and external peer and the no form of the command resets the Non BGP routes advertisement policy to default. By default, the non BGP routes are advertised to internal and external peers.

bgp nonbgproute-advt <external|both>

no bgp nonbgproute-advt

Syntax Description	**external**	-	Denotes that the non-BGP routes need to be advertised to external peers
	both	-	Determines that the non-BGP routes need to be advertised to both internal and external peers
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults	both		
Example	`iss(config-router)# bgp nonbgproute-advt both`		

☞

- The Administrator can effectively control the advertisement of the route learnt through Redistribution
- BGP Speaker Local AS number must be configured

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp info** – Displays the general info about BGP protocol
- **show running-config bgp** - Displays the current operating configuration in the system.

45.25 redistribute

This command configures the protocol from which the routes have to be redistributed into BGP after applying the specified route map. The no form of the command disables the redistribution of routes from the given protocol into BGP. The route map is disassociated from the redistribution, if the no form of the command specifies the route map.

```
redistribute <static|connected|rip|ospf|all> [route-map <string(20)>]
```

```
no redistribute <static|connected|rip|ospf|all> [route-map <string(20)>]
```

Syntax Description

static	-	Advertises routes, configured statically, in the BGP routing process
connected	-	Advertises directly connected networks routes, in the BGP routing process
rip	-	Advertises routes, that are learnt by the RIP process, in the BGP routing process
ospf	-	Advertises routes, that are learnt by the BGP process, in the BGP routing process
all	-	Advertises routes, that are learnt by the all processes (RIP ,OSPF, statically configured and connected routes), in the BGP routing process
route-map	-	Specifies the name of the Route Map to be applied during redistribution of routes to BGP. If this is not specified, all routes are redistributed. This value is a string of size 20.

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# redistribute ospf
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp info** – Displays the general info about BGP protocol

45.26 import route

This command[3] adds non-BGP IP routes into BGP.

import route ip-address prefixlen nexthop metric ifindex protocol action route-count

Syntax Description	**ip-address**	-	Prefix of the route to be imported.
	prefixlen	-	Prefix length of the route. This value ranges between 1 and 32.
	nexthop	-	Nexthop IP address for the route.
	metric	-	Metric for the route. This value ranges between 1 and 2147483647.
	ifindex	-	Interface index of the route. This value ranges between 1 and 2147483647.
	protocol	-	Protocol value for the non-BGP routes. This value can be: • 2 – Local • 3 – Static • 8 – RIP • 13 – OSPF
	action	-	Controls addition or deletion of route.
	route-count	-	Number of routes to be imported.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# import route 23.45.0.1 10 23.45.0.10 10 2 3 add 4`		

[3] This command will be effective, only if the RTM is disabled.

45.27 bgp always-compare-med

This command enables the comparison of med for routes received from different autonomous system and the no form of the command Disables the comparison of med for routes received from different autonomous system. Med will be compared only for routes from same neighbor autonomous system.

bgp always-compare-med

no bgp always-compare-med

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults Disable

Example
```
iss(config-router)# bgp always compare-med
```

☞
- BGP Speaker Local AS number must be configured
- By default in BGP route selection algorithm, MED attributes are compared between two routes only if both the routes are received from the same autonomous system. Administrator can change this default behavior by enabling always-compare-med option. If this option is enabled, then in BGP route selection algorithm, MED attributes are compared between routes even if they are received from different autonomous systems

Related Commands
- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp info** – Displays the general info about BGP protocol

45.28 default-metric

This command configures the Default IGP Metric value and the no form of the command resets the Default IGP Metric value.

default-metric <Default Metric Value>

no default-metric

Mode	Router Configuration Mode
Package	Enterprise and Metro
Defaults	0
Example	`iss(config-router)# default-metric 300`

☞

- This command sets the default metric to be associated with all redistributed routes. If a metric value is not supplied, the default metric value is assigned as 0. If the default metric value is 0, then the received route-metric is advertised. Any non-zero metric value is used as the metric value for all the redistributed routes. The metric of redistributed Local Routes is not affected by the default-metric value
- BGP Speaker Local AS number must be configured

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp info** – Displays the general info about BGP protocol

45.29 bgp med

This command configures an entry in MED Table and the no form of the command deletes the entry from MED Table.

```
bgp med <1-100> remote-as <0-65535> <ip-address> <prefixlen> [intermediate-as
<AS-no list- AS1,AS2,...>] value <value> direction <in|out> [override]
```

```
no bgp med <1-100>
```

Syntax Description

remote-as	-	AS number of BGP peer associated with the route-prefix
ip-address	-	Route-prefix on which MED policy needs to be applied
prefixlen	-	Length (in bits) of the IP address prefix in the network layer reachability information field. This value ranges between 0 and 32.
intermediate-as	-	The sequence of intermediate Autonomous system numbers through which the route update is expected to travel
value	-	Value assigned to the MED attribute
direction	-	Direction of application of med policy • Incoming - On received route-update with other matching attributes like as-number, intermediate-as numbers • Outgoing - On route-update that needs to be advertised to peer
override	-	This setting decides whether configured MED value will override the received MED value

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults

Prefixlen	-	0
direction	-	In
med	-	0

Example

```
iss(config-router)# bgp med 5 remote-as 200 212.23.45.0 24
intermediate-as 150 value 50 direction in override
```

☞
- BGP Speaker Local AS number must be configured.
- The entry will not be matched when the MED value for an update is calculated, if the prefix length is set as zero.

Related Commands

- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`show ip bgp med`** – Displays the contents of MED table
- **`show running-config bgp`** - Displays the current operating configuration in the system

45.30 bgp local-preference

This command configures an entry in the Local Preference Table and the no form of the command deletes the entry from Local Preference Table.

```
bgp local-preference <1-100> remote-as <0-65535> <ip-address> <prefixlen>
[intermediate-as <AS-no list- AS1,AS2,...>] value <value> direction <in|out>
[override]
```

```
no bgp local-preference <1-100>
```

Syntax Description	**remote-as**	-	AS number of BGP peer associated with the route-prefix
	ip-address	-	Route-prefix on which local-preference policy needs to be applied
	prefixlen	-	Length (in bits) of the IP address prefix in the network layer reachability information field. This value ranges between 0 and 32.
	intermediate-as	-	The sequence of intermediate Autonomous system numbers through which the route update is expected to travel
	value	-	The local-preference value that needs to be associated with the route-update
	direction	-	Direction of application of local-preference policy • Incoming - On received route-update with other matching attributes like as-number, intermediate-as numbers • Outgoing - On route-update that needs to be advertised to peer
	override	-	This setting decides whether configured local-preference value overrides the received local-preference value. If this keyword is not specified, then the received value will have precedence over configured value
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults	remote-as	-	0
	Direction	-	in
	Value	-	100
	ip-address	-	0.0.0.0

prefixlen - 0

Example

```
iss(config-router)# bgp local-preference 5 remote-as 200
21.3.0.0 16 intermediate-as 150 value 250 direction out override
```

- BGP Speaker Local AS number must be configured.
- The entry will not be matched when the local preference value for an update is calculated, if the prefix length is set as zero.

Related Commands

- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`show ip bgp local-pref`** – Displays the contents of local preference table
- **`show running-config bgp`** - Displays the current operating configuration in the system.

45.31 bgp update-filter

This command configures an entry in Update Filter Table and the no form of the command deletes the entry from Update Filter Table.

```
bgp update-filter <1-100> <permit|deny> remote-as <0-65535> <ip-address>
<prefixlen> [intermediate-as <AS-no list-AS1,AS2,...>] direction <in|out>
```

```
no bgp update-filter <1-100>
```

Syntax Description

permit	-	Allow route to pass filter policy test
deny	-	Filter routes when it passes through filter policy test
remote-as	-	AS number of BGP peer associated with the route-prefix
ip-address	-	Route-prefix on which Filter policy needs to be applied
prefixlen	-	Length (in bits) of the IP address prefix in the network layer reachability information field. This value ranges between 0 and 32.
intermediate-as	-	The sequence of intermediate Autonomous system numbers through which the route update is expected to travel
direction	-	Direction of application of med policy • **in** - On received route-update with other matching attributes like as-number, intermediate-as nos • **out** - On route-update that needs to be advertised to peer

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults

remote-as	-	0
direction	-	In
ip-address	-	0.0.0.0
prefixlen	-	0

Example

```
iss(config-router)# bgp update-filter 6 deny remote-as 145
72.93.0.0 14 intermediate-as 150 direction in
```

☞
- BGP Speaker Local AS number must be configured
- The NLRI field will not be matched if the prefix length is set as zero.

Related Commands

- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`show ip bgp filters`** – Displays the contents of filter table
- **`show running-config bgp`** - Displays the current operating configuration in the system.

45.32 aggregate-address index

This command configures an entry in Aggregate Table and the no form of the command sets the **AdminStatus** as **down**.

```
aggregate-address index <1-100> <ip-address> <prefixlen> [summary-only]

no aggregate-address index <1-100>
```

Syntax Description

ip-address	-	The Aggregate address
prefixlen	-	Length (in bits) of the IP address prefix in the network layer reachability information field. This value ranges between 0 and 32. The prefix length is set as zero, if values other than the range is provided.
summary-only	-	Creates an aggregated route for advertisement to peers and also suppresses the advertisement of more-specific routes to the peers

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# aggregate-address index 1 21.1.0.0 16
summary-only
```

☞

- BGP Speaker Local AS number must be configured
- The IP address and the prefix length can be configured, only if the admin status of the BGP is down.
- This command configures the (aggregation policy) route details for forming an aggregated route and creates an entry in the aggregation table. When summary-only is given, then, aggregated route alone will be sent to the peers. Otherwise, both more-specific and aggregated route are advertised

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp aggregate** – Displays the contents of aggregate table
- **show running-config bgp** - Displays the current operating configuration in the system.

45.33 bgp cluster-id

This command configures the Cluster ID for Route Reflector and the no form of the command resets the Cluster ID for Route Reflector.

bgp cluster-id <cluster id value(ip_address)>

no bgp cluster-id

Syntax Description	**cluster id value**	-	The cluster ID associated with the route-reflector

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# bgp cluster-id 10.0.0.1
```

☞ BGP Speaker Local AS number must be configured

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp rfl info** – Displays info about RFL feature

45.34 bgp client-to-client reflection

This command configures the Route Reflector to support route reflection to Client Peers and the no form of the command configures the Route Reflector not to reflect routes to Client Peers.

bgp client-to-client reflection

no bgp client-to-client reflection

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# bgp client-to-client reflection
```

☞

- BGP Speaker Local AS number must be configured
- BGP Cluster-id must be configured
- By default, Route Reflector will reflect routes learnt from a client peer to all other client peers. If required, administrator can disable this feature by disabling client-to-client reflection. If disabled, then Route Reflector will not advertise routes learnt from a client peer to other client peers. This occurs when all peers within a cluster are fully-meshed and the client peer itself is able to advertise routes to other clients of the route-reflector

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp rfl info** – Displays info about RFL feature

45.35 neighbor - route-reflector-client

This command configures the Peer as Client of the Route Reflector and the no form of the command resets the Peer as conventional BGP Peer.

neighbor <ip-address | peer-group-name> route-reflector-client

no neighbor <ip-address | peer-group-name> route-reflector-client

Syntax Description	**ip-address**	-	Peer's Remote IP address
	peer-group-name	-	Name of a BGP peer group. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
	route-reflector-client	-	Specifies the BGP peer as a client of the Route-Reflector
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# neighbor 23.45.0.1 route-reflector-client`		

☞

Related Commands

- BGP Speaker Local AS number must be configured
- Route Reflector must be enabled
- Peer must be created and peer AS must be configured
- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp rfl info** – Displays info about RFL feature
- **show running-config bgp** - Displays the current operating configuration in the system

45.36 bgp comm-route

This command configures an entry in additive or delete community table and the no form of the command removes the entry from additive or delete community table.

bgp comm-route {additive|delete} <ip-address> <prefixlen> comm-value <4294967041-4294967043,65536-4294901759>

no bgp comm-route {additive|delete} <ip-address> <prefixlen> comm-value <4294967041-4294967043,65536-4294901759>

Syntax Description

additive	-	Add associated community value with the already existing communities in the route update
delete	-	Remove the community attribute from the route-prefix when it passes through the filter process
ip-address	-	Route prefix on which community policy needs to be applied
prefixlen	-	IP prefix length for the destination. This value ranges between 1 and 32.
comm-value	-	Community attribute value

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# bgp comm-route additive 24.5.0.0 16 comm-value 4294967043
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp community** – Displays the contents of route/peer/filter/policy community tables
- **show running-config bgp** - Displays the current operating configuration in the system

45.37 bgp comm-filter

This command allows/filters the community attribute while receiving or advertising. The no form of the command removes the filter policy for the community attribute.

```
bgp comm-filter <comm-value(4294967041-4294967043,65536-4294901759)>
<permit|deny> <in|out>

no bgp comm-filter <comm-value(4294967041-4294967043,65536-4294901759)>
<permit|deny> <in|out>
```

Syntax Description

comm.-value	-	Community Attribute Value
permit	-	Allows a particular community attribute to be received or advertised in updates
deny	-	Filters routes containing the community attribute value in received or advertised updates
in|out	-	Specifies the direction of route-updates on which the community filter policy needs to be applied, i.e. whether the community filter needs to be applied on received routes or on routes advertised to peers

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# bgp comm-filter 75100 deny in
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp community** – Displays the contents of route/peer/filter/policy community tables

45.38 bgp comm-policy

This command configures the community attribute advertisement policy for specific destination. The no form of the command removes the community attribute advertisement policy for specific destination.

bgp comm-policy <ip-address> <prefixlen> <set-add|set-none|modify>

no bgp comm-policy <ip-address> <prefixlen>

Syntax Description	**ip-address**	-	Route prefix on which community policy needs to be applied
	prefixlen	-	IP prefix length of the destination. This value ranges between 0 and 32.
	set-add	-	Sends only the configured additive communities with associated route
	set-none	-	Sends the associated route without any communities
	modify	-	Removes the associated route with received delete communities and adds the configured additive communities
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# bgp comm-policy 24.5.0.0 10 set-none`		
☞	BGP Speaker Local AS number must be configured.		
Related Commands	• **router bgp** – Sets the AS number of the BGP Speaker • **show ip bgp community policy**– Displays the contents of policy community tables • **show running-config bgp** - Displays the current operating configuration in the system		

45.39 bgp ecomm-route

This command configures an entry in additive or delete ext community table. The no form of the command removes the entry from additive or delete ext community table.

bgp ecomm-route {additive|delete} <ip-address> <prefixlen> ecomm-value <value(xx:xx:xx:xx:xx:xx:xx:xx)>

no bgp ecomm-route {additive|delete} <ip-address> <prefixlen> ecomm-value <value(xx:xx:xx:xx:xx:xx:xx:xx)>

Syntax Description	**additive**	-	Adds associated extended-community value with the already existing communities in the route update
	delete	-	Removes the extended-community attribute from the route-prefix when it passes through the filter process
	ip-address	-	Route prefix on which extended-community policy needs to be applied
	prefixlen	-	IP prefix length of the destination. This value ranges between 0 and 32.
	ecomm-value	-	Extended Community Attribute Value

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# bgp ecomm-route additive 12.0.0.0 2 ecomm-value 01:01:22:33:44:55:66:77
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **show ip bgp extcommunity route** – Displays the contents of route ext-community route tables
- **show running-config bgp** - Displays the current operating configuration in the system
- **router bgp – Sets the AS number of the BGP Speaker**

45.40 bgp ecomm-filter

This command allows/filters the ext community attribute while receiving or advertising. The no form of the command removes the filter policy for the ext community attribute.

bgp ecomm-filter <ecomm-value(xx:xx:..:xx)> <permit|deny> <in|out>

no bgp ecomm-filter <ecomm-value(xx:xx:..:xx)> <permit|deny> <in|out>

Syntax Description	**ecomm-value**	-	The extended community value
	permit	-	Allows the route -update with the associated extended community value to pass the filter test
	deny	-	Denies the route-update with the associated extended community value to pass the filter test
	in	-	Incoming direction of applied filter
	out	-	Outgoing direction of applied filter

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# bgp ecomm-filter 01:01:22:33:23:43:44:22 deny
in
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp extcommunity** – Displays the contents of route/peer/filter/policy ext-community route table

45.41 bgp ecomm-policy

This command configures the extended community attribute advertisement policy for specific destination. The no form of the command removes the extended community attribute advertisement policy for specific destination.

bgp ecomm-policy <ip-address> <prefixlen > <set-add|set-none|modify>

no bgp ecomm-policy <ip-address> <prefixlen>

Syntax Description	**ip-address**	-	The route prefix on which extended community policy needs to be applied
	prefixlen	-	IP prefix length of the destination. This value ranges between 0 and 32.
	set-add	-	Sends associated route with configured additive extended-communities only
	set-none	-	Sends the associated route without any extended-communities
	modify	-	Strips the associated route with received delete extended communities and adds the configured additive extended communities

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# bgp ecomm-policy 12.0.0.0 14 set-add
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp extcommunity policy** – Displays the contents of policy ext-community route tables
- **show running-config bgp** - Displays the current operating configuration in the system

45.42 bgp confederation identifier

This command specifies the BGP confederation identifier. The no form of the command removes the BGP confederation identifier.

bgp confederation identifier <AS no(1-65535)>

no bgp confederation identifier

Mode Router Configuration Mode

Package Enterprise and Metro

Example
```
iss(config-router)# bgp confederation identifier 1000
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp confed info** – Displays info about confederation feature

45.43 bgp confederation peers

This command configures the Autonomous Systems that belongs to the confederation. The no form of the command removes the Autonomous Systems from the confederation.

bgp confederation peers <AS no(1-65535)>

no bgp confederation peers <AS no(1-65535))

Mode	Router Configuration Mode
Package	Enterprise and Metro
Example	`iss(config-router)# bgp confederation peers 100`

☞

Related Commands

- BGP Speaker Local AS number must be configured
- The peer AS number must not be equal to BGP Speaker Local AS number
- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp confed info** – Displays info about confederation feature

45.44 bgp bestpath med confed

This command enables MED comparison among paths learnt from confed peers. The no form of the command disables MED comparison among paths learnt from confed peers.

bgp bestpath med confed

no bgp bestpath med confed

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# bgp bestpath med confed
```

☞

- BGP Speaker Local AS number must be configured
- By default, in BGP route selection algorithm, MED attributes comparison between two routes originated within the local confederation is disabled. Enabling this option, will allow the router to compare MED attribute between routes originated from the local confederation

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp confed info** – Displays info about confederation feature

45.45 neighbor - password

This command configures the password for TCP-MD5 authentication with peer. The no form of the command resets the TCP-MD5 password set for the peer.

neighbor <ip-address> password password-string

no neighbor <ip-address> password

Syntax Description	**ip-address**	-	IP address of the BGP peer
	password	-	The password that needs to be used for TCP-MD5 authentication with the peer
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# neighbor 10.0.0.2 password abcdef`		

☞

Related Commands

- BGP Speaker Local AS number must be configured
- Peer must have been created
- **router bgp** – Sets the AS number of the BGP Speaker
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **show ip bgp info** – Displays the general info about BGP protocol

45.46 import ipv6-route

This command[3] adds non-BGP IPv6 routes into BGP.

import ipv6-route ip-address prefixlen nexthop metric ifindex protocol action route-count

Syntax Description	**ip-address**	-	Prefix of the route to be imported.
	prefixlen	-	Prefix length of the route. This value ranges between 1 and 32.
	nexthop	-	Nexthop IP address for the route.
	metric	-	Metric for the route. This value ranges between 1 and 2147483647.
	ifindex	-	Interface index of the route. This value ranges between 1 and 2147483647.
	protocol	-	Protocol value for the non-BGP routes. This value can be: • 2 – Local • 3 – Static • 8 – RIP • 13 – OSPF
	action	-	Controls addition or deletion of route.
	route-count	-	Number of routes to be imported.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# import ipv6-route 23.45.0.1 10 23.45.0.10 10 2 3 add 4`		

45.47 address-family

This command puts the router into the address-family command mode. The no form of the command disables the address-family command mode and deletes the peers belonging to the IPV4, IPv6 and VPNv4 address family.

```
address-family [ipv4 | ipv6]
```

```
no address-family { ipv4 | ipv6}
```

Syntax Description	**ipv4**	-	Configure session that carries standard IPv4 address prefixes.
	ipv6	-	Configure session that carries standard IPv6 address prefixes.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults	Routing information is advertised for IPv4 address family when a BGP session is configured, unless the default advertising is reset.		
Example	`iss(config-router)# address-family ipv6`		
Related Commands	• **router bgp** – Sets the AS number of the BGP Speaker • **show ip bgp** – Displays the BGP related information		

45.48 bgp graceful-restart

This command enables the graceful restart capability. The no form of the command disables the graceful restart capability and resets the restart-time or stalepath-time to default value.

bgp graceful-restart [restart-time <(1-4096)<seconds>] [stalepath-time <(90-3600)<seconds>]

no bgp graceful-restart [restart-time] [stalepath-time]

Syntax Description	**restart-time**	-	Estimated time (in seconds) to be taken for re-establishing a BGP session after restart. This value ranges between 1 and 4096 seconds.
	stalepath-time	-	Time (in seconds) until which the router retains the stale routes. This value ranges between 90 and 3600 seconds.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults	restart-time	-	90
	stalepath-time	-	150

Example

```
iss(config-router)# bgp graceful-restart restart-time 2000
stalepath-time 300
```

☞

- BGP Speaker Local AS number should be configured
- The default value of the restart time will be less than or equal to hold time carried in open message.

Related Commands

- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`shutdown ip bgp`** – Sets the BGP Speaker Global Admin status DOWN
- **`show ip bgp restartexitreason`** - Displays the restart exit reason of the BGP
- **`show ip bgp restartstatus`** - Displays the restart status of the BGP
- **`show ip bgp info`** – Displays the general info about BGP protocol
- **`show ip bgp timers`** - Displays the value of BGP timers
- **`show running-config bgp`** - Displays the current operating configuration in the system

45.49 bgp update-delay

This command configures the selection deferral time interval. This time interval represents the time (in seconds) until which the router defers its route selection. This value ranges between 60 and 1800 seconds.

This time interval should be configured to provide enough time for all the peers of the restarting speaker to send all the routes to the restarting speaker.

The no form of the command resets the time interval to the default value.

bgp update-delay <(60-1800)seconds>

no bgp update-delay

Mode	Router Configuration Mode
Package	Enterprise and Metro
Defaults	60
Example	`iss(config-router)# bgp update-delay 90`
☞	• BGP Speaker Local AS number should be configured • The selection deferral time interval can be configured, only if the BGP Speaker GR Admin Status is disabled.
Related Commands	• **router bgp** – Sets the AS number of the BGP Speaker • **shutdown ip bgp** – Sets the BGP Speaker Global Admin status DOWN • **show ip bgp timers** - Displays the value of BGP timers

45.50 restart-support

This command enables the graceful restart support. Graceful restart support is provided for both planned and unplanned restart, if the command is executed without any option.

The no form of the command disables the graceful restart support.

```
restart-support [plannedOnly]
```

```
no restart-support
```

Syntax Description	**plannedOnly**	-	Supports only the planned restarts (such as restarting a control plane after a planned downtime).

Mode Router Configuration Mode

Package Enterprise and Metro

Defaults Graceful restart support is disabled.

Example

```
iss(config-router)# restart-support
```

☞
- BGP Speaker Local AS number should be configured
- The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

Related Commands
- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`show ip bgp restartsupport`** - Displays the restart support of the BGP

45.51 restart-reason

This command configures the reason for BGP graceful restart. The no form of the command resets the reason for restart.

restart-reason [{unknown|softwareRestart|swReloadUpgrade}]

no restart-reason [{unknown|softwareRestart|swReloadUpgrade}]

Syntax Description	**unknown**	-	System restarts due to unplanned events (such as restarting after a crash).
	softwareRestart	-	System restarts due to software restart.
	swReloadUpgrade	-	System restarts due to reloading / upgrading of software.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults	softwareRestart		
Example	`iss(config-router)# restart-reason swReloadUpgrade`		

☞

- BGP Speaker Local AS number should be configured
- The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **show ip bgp restartreason** - Displays the restart reason of the BGP

45.52 distribute-list route-map

This command enables route map filtering for inbound or outbound routes. The no form of the command disables route map filtering for inbound or outbound routes.

```
distribute-list route-map <name(1-20)> {in | out}
```

```
no distribute-list route-map <name(1-20)> {in | out}
```

Syntax Description	**name**	-	Specifies the name of the Route Map for which filtering should be enabled. This value is a string of size 20.
	in	-	Sets filtering for inbound routes.
	out	-	Sets filtering for outbound routes.

Mode Router Configuration Mode

Package Enterprise and Metro

Example

```
iss(config-router)# distribute-list route-map rmap-test in
```

☞

- BGP Speaker Local AS number should be configured
- Only one route map can be set for inbound or outbound routes. Another route map can be assigned, only if the already assigned route map is disabled.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker

45.53 distance

This command enables the administrative distance (that is, the metric to reach destination) of the routing protocol and sets the administrative distance value. The distance value ranges between 1 and 255.

The administrative distance can be enabled for only one route map. The distance should be disabled for the already assigned route map, if distance needs to be enabled for another route map.

The no form of the command disables the administrative distance.

```
distance <1-255> [route-map <name(1-20)>]
```

```
no distance [route-map <name(1-20)>]
```

Syntax Description	**name**	-	Name of the Route Map for which the distance value should be enabled and set. This value is a string of size 20.
Mode	Router Configuration Mode		
Package	Enterprise and Metro		
Defaults	122		
Example	`iss(config-router)# distance 10 route-map rmap-test`		

☞ **Related Commands**

- BGP Speaker Local AS number should be configured
- **`router bgp`** – Sets the AS number of the BGP Speaker

45.54 clear ip bgp

This command resets the bgp connection dynamically for inbound and outbound route policy.

```
clear ip bgp {* | <ip-address|peer-group-name>} [soft {in|out}]
```

Syntax Description

*****	-	All BGP peers
ip-address	-	Remote IP address associated with specific BGP peer
peer-group-name	-	Name of a BGP peer group. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
soft	-	Soft clear
in	-	Initiates inbound soft reconfiguration
out	-	Initiates outbound soft configuration

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# clear ip bgp 12.0.0.1
```

☞ If the keyword soft and the associated direction are not specified, then this causes hard clear, that is, the BGP session with peer is reset.

Related Command **show ip bgp** – Displays the BGP related information

45.55 clear bgp ipv6

This command dynamically resets the BGPv6 connection for inbound / outbound route policy.

```
clear bgp ipv6 <*| ip-address |peer-group-name> [soft <in|out>]
```

Syntax Description

*****	- All BGP peers
ip-address	- Remote IP address associated with specific BGP peer
peer-group-name	- Name of a BGP peer group. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
soft	- Initiates soft reset (that is, the BGP session with peer is not reset). The available options are: • in – Performs a dynamic soft inbound reset • out – Performs a dynamic soft outbound reset

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# clear bgp ipv6 12.0.0.1
```

☞ If the keyword soft and the associated direction are not specified, then this causes hard clear (that is, the BGP session with peer is reset).

Related Command

- **show ip bgp** – Displays the BGP related information
- **show ip bgp summary** - Displays the status of all BGP4 connections

45.56 shutdown ip bgp

This command sets the BGP Speaker Global Admin status DOWN and the no form of the command sets the BGP Speaker Global Admin status UP.

shutdown ip bgp

no shutdown ip bgp

Mode Global Configuration Mode

Package Enterprise and Metro

Example

```
iss(config)# shutdown ip bgp
```

☞ The shutdown command does not affect all the configurations. All peer sessions go down and routes learnt through redistribution are lost. If RFD is enabled, then routes history is cleared.

Related Commands

- **ip bgp overlap-policy** – Configures the Overlap Route policy for the BGP Speaker
- **ip bgp synchronization / synchronization** – Enables synchronization between BGP and IGP
- **show ip bgp info** – Displays the general info about BGP protocol

45.57 debug ip bgp

This command configures the Trace levels. The no form of the command resets the Trace levels.

debug ip bgp {peer | update | fdb | keep | in | out | damp | events | gr | all }

no debug ip bgp {peer | update | fdb | keep | in | out | damp | events | gr | all}

Syntax Description

peer	-	Trace code related to peer processing
update	-	Trace code related to update processing
fdb	-	Trace code related to FIB updation
keep	-	Trace code related to keep-alives
in	-	Trace code related to incoming messages
out	-	Trace code related to outgoing messages
damp	-	Trace code related to dampening parameters
events	-	Trace code related to BGP event processing
gr	-	Trace code related to graceful restart
all	-	All the BGP trace code

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# debug ip bgp peer
```

- The autonomous number and the router ID must be set for the router before configuring the trace levels.

Related Commands

- **as-num** - Sets the autonomous number for the router.
- **router-id** - Sets the router ID's address for the router.

45.58 show bgp-version

This command displays the BGP Version information.

show bgp-version

Mode	Privileged EXEC Mode
Package	Enterprise and Metro
Example	`iss# show bgp-version` `Interface MastersBGP Version : 4`
☞	BGP Speaker Local AS number must be configured.
Related Command	**router bgp** – Sets the AS number of the BGP Speaker

45.59 show ip bgp

This command displays the BGP related information.

show ip bgp {[neighbor [<peer-addr>]] | [rib] | [stale]}

Syntax Description

neighbor	-	IP address of the neighbor.
rib	-	BGP local RIB (Routing Information Base).
stale	-	Routes gone stale due to Graceful restart.

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp neighbor 60.0.0.5

BGP neighbor is 60.0.0.5, remote AS 500, external link
  BGP version 4, remote router ID 60.0.0.5
  BGP state = Established, up for 2 minutes 47 seconds
  Rcvd update before 0 secs, hold time is 90, keepalive interval
is 30 secs
  Neighbors Capability:
    Route-Refresh: Advertised and received
    Address family IPv4 Unicast: Advertised and received
  Received 7 messages, 0 Updates
  Sent 7 messages, 1 Updates
  Route refresh: Received 0, sent 0.
  Minimum time between advertisement runs is 30 seconds
  Connections established 1 time(s)
  Local host: 60.0.0.2, Local port: 179
  Foreign host: 60.0.0.5, Foreign port: 49152
  Last Error: Code 0, SubCode 0.


iss# show ip bgp rib

BGP table version is 1,local router ID is 60.0.0.2
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Type  Network        NextHop        Metric LocPrf Path Origin
   ----  -------        -------        ------ ------ ---- ------
   >    66.0.0.0/8      60.0.0.66/4      0      -      ?
```

```
iss# show ip bgp stale

BGP table version is 7,local router ID is 60.0.0.5
Origin codes: i - IGP, e - EGP, ? - incomplete

 Network             NextHop           Metric LocPrf Path Origin
--------             -------           ------ ------ ---- ------
66.0.0.0/8      60.0.0.66/4              100    200      ?
```


BGP Speaker Local AS number must be configured.

Related Commands

- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`bgp router-id`** – Configures the BGP Identifier of the BGP Speaker
- **`neighbor - shutdown`** – Disables the Peer session
- **`neighbor - update-source`** - Configures the source-address for routing updates and for TCP connection establishment with a peer
- **`neighbor - gateway`** - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer
- **`neighbor - remote-as`** – Creates a Peer and initiates the connection to the peer
- **`clear ip bgp`** – Resets the BGP connection dynamically for inbound and outbound route policy

45.60 show ip bgp restart mode

This command displays the restart mode of the BGP router and neighbors.

show ip bgp {restartmode [neighbor [<peer-addr>]]}

Syntax Description	**neighbor**	-	IP address of the neighbor
Mode	Privileged EXEC Mode		
Package	Enterprise and Metro		
Example	iss# show ip bgp restartmode Interface Masters BGP4:- In Receiving Mode iss# show ip bgp restartmode Interface Masters BGP4:- In Restarting mode		
Related Commands	**neighbor - remote-as** - Creates a Peer and initiates the connection to the peer		

45.61 show ip bgp EndOfRIBMarkerStatus

This command displays the End_Of_RIB marker status of the BGP router and neighbors.

show ip bgp {EndOfRIBMarkerStatus [neighbor [<peer-addr>]]}

Syntax Description

neighbor	-	IP address of the neighbor

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp EndOfRIBMarkerStatus
 Neighbor    EORSent EORRcvd
 ---------   ------- -------
  60.0.0.5    NA      Received
  30.0.0.4    Sent    Received


iss# show ip bgp EndOfRIBMarkerStatus neighbor 60.0.0.5
 Neighbor    EORSent EORRcvd
 ---------   ------- -------
  60.0.0.5    NA      Received
```

Related Commands **neighbor - remote-as** - Creates a Peer and initiates the connection to the peer

45.62 show ip bgp restartreason

This command displays the restart reason of the BGP.

show ip bgp restartreason

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp restartreason
Interface Masters BGP4: Restart reason is software restart

iss# show ip bgp restartreason
Interface Masters BGP4: Restart reason is software upgrade

iss# show ip bgp restartreason
Interface Masters BGP4: Restart reason is unknown
```

Related Commands **restart-reason** – Configures the reason for BGP graceful restart

45.63 show ip bgp restartexitreason

This command displays the restart exit reason of the BGP.

show ip bgp restartexitreason

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp restartexitreason
Interface Masters BGP4: Restart In Progress

iss# show ip bgp restartexitreason
Interface Masters BGP4: Speaker has not restarted

iss# show ip bgp restartexitreason
Interface Masters BGP4: GR Exit Reason is Success

iss# show ip bgp restartexitreason
Interface Masters BGP4: GR Exit Reason is Failure
```

Related Commands

- **neighbor – remote-as** – Creates a Peer and initiates the connection to the peer
- **bgp graceful-restart** - Enables the graceful restart capability

45.64 show ip bgp restartsupport

This command displays the restart support of the BGP.

show ip bgp restartsupport

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp restartsupport
Interface Masters BGP4: Both planned and unplanned restart are
supported
```

```
iss# show ip bgp restartsupport
Interface Masters BGP4: Planned restart is supported
```

```
iss# show ip bgp restartsupport
Interface Masters BGP4: Speaker does not have restart support
```

Related Commands

- **neighbor – remote-as** – Creates a Peer and initiates the connection to the peer
- **restart-support** - Enables the graceful restart support

45.65 show ip bgp restartstatus

This command displays the restart status of the BGP.

show ip bgp restartstatus

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp restartstatus
Interface Masters BGP4: Restart status in none
```

```
iss# show ip bgp restartstatus
Interface Masters BGP4: Restart status is unplanned
```

```
iss# show ip bgp restartstatus
Interface Masters BGP4: Restart status is planned
```

Related Commands

- **neighbor – remote-as** – Creates a Peer and initiates the connection to the peer
- **bgp graceful-restart** - Enables the graceful restart capability

45.66 show ip bgp community - routes

This command displays routes that belong to specified BGP communities.

show ip bgp community community-number(4294967041-4294967043,65536-4294901759) [exact]

Syntax Description	**community-number**	-	BGP Community attribute
	exact	-	Displays the routes that has the same specified communities
Mode	Privileged EXEC Mode		
Package	Enterprise and Metro		

Example

```
iss# show ip bgp community 75000

BGP table version is 5,local router ID is 10.0.0.2
Status codes: d damped * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop    Metric LocPrf Path
-------          ---- ---    ------ ------ ----
76.0.0.0/8        10.0.0.1       1        100
77.0.0.0/8        10.0.0.1       1        100
78.0.0.0/8        10.0.0.1       1        100

iss# show ip bgp community 75000 exact

BGP table version is 5,local router ID is 10.0.0.2
Status codes: d damped * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop    Metric LocPrf Path
-------          ---- ---    ------ ------ ----
76.0.0.0/8        10.0.0.1       1        100
77.0.0.0/8        10.0.0.1       1        100
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **bgp comm-policy** – Configures the community attribute advertisement policy for specific destination
- **bgp comm-filter** – Allows/filters the community attribute while receiving or advertising
- **bgp comm-route** – Configures an entry in additive or delete community table

45.67 show ip bgp extcommunity - routes

This command displays routes that belong to specified BGP extended-communities.

show ip bgp extcommunity <value(xx:xx:xx:xx:xx:xx:xx:xx)> [exact]

Syntax Description	**exact**	- Displays the routes that has the same specified extended communities

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp extcommunity 01:02:33:33:33:33:33:33

BGP table version is 5,local router ID is 10.0.0.2
Status codes: d damped * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop    Metric LocPrf Path
-------          ---- ---    ------ ------ ----
75.0.0.0/8        10.0.0.1      1        100
79.0.0.0/8        10.0.0.1      1        100


iss# show ip bgp extcommunity 01:02:33:33:33:33:33:33 exact

BGP table version is 5,local router ID is 10.0.0.2
Status codes: d damped * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network        Next Hop    Metric LocPrf Path
-------          ---- ---    ------ ------ ----
75.0.0.0/8        10.0.0.1      1        100
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **`router bgp`** – Sets the AS number of the BGP Speaker
- **`bgp ecomm-route`** – Configures an entry in additive or delete extended community table
- **`bgp ecomm-filter`** – Allows/filters the extended community attribute while receiving or advertising
- **`bgp ecomm-policy`** – Configures the extended community attribute advertisement policy for specific destination

45.68 show ip bgp summary

This command displays the status of all BGP4 connections.

show ip bgp summary

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp summary

BGP router identifier is 140.0.0.2, local AS number 200
Forwarding State is enabled

BGP router identifier is 140.0.0.2, local AS number 200

 BGP table version is 0
 Neighbor  Version  AS  MsgRcvd  MsgSent  Up/Down  State/PfxRcd
 --------- -------  --  -------  -------  -------  ------------
  60.0.0.5    4    500     26       25   00:00:12:15 Established
```

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **ip bgp dampening** – Configures the Dampening Parameters
- **ip bgp overlap-policy**– Configures the Overlap Route policy for the BGP Speaker
- **bgp router-id** – Configures the BGP Identifier of the BGP Speaker
- **bgp default local-preference** – Configures the Default Local Preference value
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **no ip bgp overlap-policy** – Resets the Overlap route policy to default

45.69 show ip bgp filters

This command displays the contents of filter table.

show ip bgp filters

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp filters

Index AdminStatus Remote-AS Prefix PrefixLen Inter-AS Direction Action
    ----- ----------- --------- ------ --------- -------- --------- ------

6        up         145    72.93.0.0 16       150     in filter
```

☞ BGP Speaker Local AS number must be configured.

Related Command

- **bgp update-filter** – Configures an entry in Update Filter Table

45.70 show ip bgp aggregate

This command displays the contents of aggregate table.

show ip bgp aggregate

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp aggregate

Index AdminStatus  Prefix PrefixLen Advertise
 ----- -----------  ------ --------- ---------
 1        up         10.0.0.0  8       all
 2        up         20.0.0.0  8   summary-only
 3        up         50.0.0.0  8       all
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **aggregate-address index** – Configures an entry in Aggregate Table

45.71 show ip bgp med

This command displays the contents of MED table.

show ip bgp med

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp med

Index Admin  Remote-AS Prefix PrefixLen Inter-AS Direction Value Preference
      Status
----- ------ --------- ------ --------- -------- --------- ----- ----------

5        up    200  212.23.45.0 24       150      in      50   true
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **bgp med** – Configures an entry in MED Table
- **bgp bestpath med confed** – Enables MED comparison among paths learnt from confed peers

45.72 show ip bgp dampening

This command displays the contents of dampening table.

show ip bgp dampening

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp dampening

Half Life Time is 900
Reuse value is 500
Suppress value is 3500
Max Suppress time is 3600
Decay timer granularity is 1
Reuse timer granularity is 15
Reuse index array size is 1024
```

☞ BGP Speaker Local AS number must be configured.

Related Command

- **ip bgp dampening** – Configures the Dampening Parameters

45.73 show ip bgp local-pref

This command displays the contents of local preference table.

show ip bgp local-pref

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp local-pref

Index Admin  Remote-AS Prefix PrefixLen Inter-AS Direction Value Preference
      Status
----- ------ --------- ------ --------- -------- --------- ----- ----------

5        up    200     21.3.0.0 16       150      in       2  false
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **bgp default local-preference** – Configures the Default Local Preference value
- **bgp local-preference** – Configures an entry in Local Preference Table

45.74 show ip bgp timers

This command displays the value of BGP timers.

show ip bgp timers

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp timers
Graceful restart Timers
------------------------
 Restart Time   90
 Stale Time     150
 Selection Deferral Timer Time  60
  Peer Timers
  Peer Address Holdtime KeepAliveTime ConnectRetry ASOrig
RouteAdvt RestartTime
  ---- ------- -------- ------------- ------------ ------ -------
-- -----------
  60.0.0.5        90        30             30       15     30
NA
```

Related Command

- **ip bgp dampening** – Configures the Dampening Parameters
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **neighbor - interval** – Configures neighbor interval
- **neighbor - timers** – Configures neighbor KeepAlive Time and Hold Time Intervals
- **bgp graceful-restart** - Enables the graceful restart capability
- **bgp update-delay** - Configures the selection deferral time interval

45.75 show ip bgp info

This command displays the general information about BGP protocol.

show ip bgp info

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp info

Routing Protocol is "bgp 200"
IGP synchronization is disabled
Both more-specific and less-specific overlap route policy is set
Local Preference is 100
Non-bgp routes are advertised to both external and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:
 BGP GR admin status is disabled

Peer Table
Peer Address RemoteAS NextHop  MultiHop send-community
---- ------- -------- ------- -------- --------------
60.0.0.5     500     automatic disable  standard,extended

 TCPMD5 Auth Table
 Peer Address Password
 ---- ------- --------
```

Related Commands

- **router bgp** – Sets the AS number of the BGP Speaker
- **ip bgp overlap-policy** – Configures the Overlap Route policy for the BGP Speaker
- **default-information originate** - enables redistribution and advertisement of the default router
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **ip bgp synchronization / synchronization** – Enables synchronization between BGP and IGP
- **bgp default local-preference** – Configures the Default Local Preference value
- **neighbor - ebgp-multihop** – Enables BGP to establish connection with external peers
- **neighbor - next-hop-self** – Enables BGP to send itself as the next hop for

advertised routes

- **neighbor – interval** – Configures neighbor interval
- **neighbor – timers** – Configures neighbor KeepAlive Time and Hold Time Intervals
- **bgp nonbgproute-advt** – Controls the advertisement of Non-BGP routes
- **redistribute** – Configures the protocol from which the routes have to be redistributed into BGP
- **bgp always-compare-med** – Enables the comparison of med for routes received from different autonomous system
- **default-metric** – Configures the Default IGP Metric value
- **neighbor – password** – Configures the password for TCP-MD5 authentication with peer
- **bgp graceful-restart** - Enables the graceful restart capability
- **shutdown ip bgp** – Sets the BGP Speaker Global Admin status DOWN

45.76 show ip bgp rfl info

This command displays information about RFL feature.

show ip bgp rfl info

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp rfl info

Cluster id is  10.0.0.1
Desired Support of the route reflector - Client Support
 BGP Peer Extension Table
 Peer Address Client/Non-Client
 ---- ------- -----------------
  10.0.0.2       Non-client
  10.0.0.3       Non-client
  10.0.0.4       Client
  10.0.0.6       Non-client
  10.0.0.7       Non-client
  10.0.0.8       Non-client
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **bgp nonbgproute-advt** – Controls the advertisement of Non-BGP routes either to the external peer (1) or both to internal & external peer (2)
- **bgp client-to-client reflection** – Configures the Route Reflector to support route reflection to Client Peers
- **neighbor - route-reflector-client** – Configures the Peer as Client of the Route Reflector
- **bgp cluster-id** – Configures the Cluster ID for Route Reflector

45.77 show ip bgp confed info

This command displays info about confederation feature.

show ip bgp confed info

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp confed info

Confederation Identifier is 1000
Confederation best path med comparision is not set
Confederation peers:  200 300 400
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **bgp confederation identifier** – Specifies the BGP confederation identifier
- **bgp bestpath med confed** – Enables MED comparison among paths learnt from confed peers
- **bgp confederation peers** – Configures the Autonomous Systems that belongs to the confederation

45.78 show ip bgp community

This command displays the contents of community tables.

show ip bgp community {route|policy|filter}

Syntax Description

route	-	Entry in additive or delete community table
policy	-	Community attribute advertisement policy for specific destination
filter	-	Filters the community attribute while receiving or advertising

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp community route

Additive Community Table
 Prefix      PrefixLen    AddCommVal
 -----       ---------    ----------

 30.0.0.0       8          70000
 60.0.0.0       8          75000
 75.0.0.0       8          70000
 76.0.0.0       8          75000
 77.0.0.0       8          75000
 78.0.0.0       8          75000
 78.0.0.0       8          76000

Delete Community Table
 Prefix      PrefixLen    DeleteCommVal
 ------      ---------    --------------

 40.0.0.0      8            80000
 70.0.0.0      8            85000

iss# show ip bgp community filter

Incoming Filter Table
 CommValue   FilterStatus
 ---------   ------------
 70000       accept
 80000       deny
Outgoing Filter Table
 CommValue   FilterStatus
```

```
 ---------  -------------
 75000      accept
 85000      deny

iss# show ip bgp community policy

Community Policy Table
 Prefix     PrefixLen   SendStatus
 ------     ---------   -----------
 20.0.0.0     8           set-add
 30.0.0.0     8           set-none
 40.0.0.0     8           modify
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **`bgp comm-route`** – Configures an entry in additive or delete community table
- **`bgp comm-filter`** – Allows/filters the community attribute while receiving or advertising
- **`bgp comm-policy`** – Configures the community attribute advertisement policy for specific destination
- **`neighbor - send-community`** – Enables advertisement of community attributes to (standard/extended) peer

45.79 show ip bgp extcommunity

This command displays the contents of ext-community tables.

show ip bgp extcommunity {route|policy|filter}

Syntax Description	**route**	-	Entry in additive or delete ext community table
	policy	-	Extended community attribute advertisement policy for specific destination
	filter	-	Filters the ext community attribute while receiving or advertising

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip bgp extcommunity route

Additive Ext-Community Table
Prefix      PrefixLen   AddEcommVal
------      ---------   -----------

30.0.0.0        8       1:1:22:33:44:55:66:77
60.0.0.0        8       1:1:22:33:44:55:66:88
75.0.0.0        8       1:1:33:33:33:33:33:33
76.0.0.0        8       1:2:44:33:33:33:33:33
78.0.0.0        8       1:2:33:33:33:33:33:33
78.0.0.0        8       1:2:33:33:33:33:33:44
79.0.0.0        8       1:2:33:33:33:33:33:44
79.0.0.0        8       1:2:33:33:33:33:33:33

Delete Ext-Community Table
Prefix      PrefixLen   DeleteEcommVal
--------    ---------   ---------------
40.0.0.0        8       1:1:55:33:44:55:66:77
70.0.0.0        8       1:1:22:33:44:55:66:99

iss# show ip bgp extcommunity filter

Incoming Filter Table
EcommValue              FilterStatus
----------              ------------
```

```
1:1:22:33:44:55:34:77      deny
1:1:22:33:44:55:66:77      accept

Outgoing Filter Table
EcommValue                FilterStatus
----------                -------------
1:1:22:33:44:55:99:77      accept
1:1:44:33:77:66:99:56      deny

iss# show ip bgp extcommunity policy

Community Policy Table
 Prefix      PrefixLen    SendStatus
 ------      ---------    -----------

 20.0.0.0      8           set-add
 30.0.0.0      8           set-none
 40.0.0.0      8           modify
```

☞ BGP Speaker Local AS number must be configured.

Related Commands

- **bgp ecomm-route** – Configures an entry in additive or delete ext community table
- **bgp ecomm-filter** – Allows/filters the ext community attribute while receiving or advertising
- **bgp ecomm-policy** – Configures the extended community attribute advertisement policy for specific destination

45.80 show bgp ipv6

This command displays the BGPv6 related information.

show bgp ipv6 {[neighbor [<peer-addr>]] | [rib] | [stale]}

Syntax Description

neighbor	-	IPv6 address of the neighbor whose related information needs to be displayed.
rib	-	BGP local RIB (Routing Information Base) related information.
stale	-	Information related to routes that have gone stale due to restart.

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
show bgp ipv6 neighbor

BGP neighbor is 2130::1, remote AS 10, external link
  BGP version 4, remote router ID 13.0.0.1
  BGP state = Established, up for 11 minutes 19 seconds
  Rcvd update before 677 secs, hold time is 90, keepalive
interval is 30 secs
  Neighbors Capability:
    Route-Refresh: Advertised and received
    Address family IPv4 Unicast: Advertised and received
  Received 24 messages, 1 Updates
  Sent 24 messages, 0 Updates
  Route refresh: Received 0, sent 0.
  Minimum time between advertisement runs is 30 seconds
  Connections established 1 time(s)
  Local host: 0.0.48.33, Local port: 49153
  Foreign host: 0.0.48.33, Foreign port: 179
  Last Error: Code 0, SubCode 0.

BGP neighbor is 2340::4, remote AS 40, external link
  BGP version 4, remote router ID 34.0.0.4
  BGP state = Established, up for 11 minutes 18 seconds
  Rcvd update before 0 secs, hold time is 90, keepalive interval
is 30 secs
  Neighbors Capability:
    Route-Refresh: Advertised and received
    Address family IPv4 Unicast: Advertised and received
  Received 23 messages, 0 Updates
  Sent 24 messages, 1 Updates
  Route refresh: Received 0, sent 0.
  Minimum time between advertisement runs is 30 seconds
```

```
  Connections established 1 time(s)
  Local host: 0.0.64.35, Local port: 179
  Foreign host: 0.0.64.35, Foreign port: 49153
  Last Error: Code 0, SubCode 0.
```

```
show bgp ipv6 neighbor 2130::1

BGP neighbor is 2130::1, remote AS 10, external link
  BGP version 4, remote router ID 13.0.0.1
  BGP state = Established, up for 12 minutes 18 seconds
  Rcvd update before 736 secs, hold time is 90, keepalive
interval is 30 secs
  Neighbors Capability:
    Route-Refresh: Advertised and received
    Address family IPv4 Unicast: Advertised and received
  Received 26 messages, 1 Updates
  Sent 25 messages, 0 Updates
  Route refresh: Received 0, sent 0.
  Minimum time between advertisement runs is 30 seconds
  Connections established 1 time(s)
  Local host: 0.0.48.33, Local port: 49153
  Foreign host: 0.0.48.33, Foreign port: 179
  Last Error: Code 0, SubCode 0.
```

```
show bgp ipv6 rib

BGP table version is 1,local router ID is 13.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Type  Network        NextHop              Metric LocPrf Path
Origin
   ----  -------        -------              ------ ------ ---- -
-----
   >    2091::/24       2130::1/16           1      100     10
?
```

```
show bgp ipv6 stale

BGP table version is 1,local router ID is 13.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

 Network        NextHop              Metric LocPrf Path Origin
  -------        -------              ------ ------ ---- ------
   2091::/24       2130::1/16           1      100     10      ?
```

Related Commands

- **neighbor – remote-as** – Creates a Peer and initiates the connection to the peer
- **neighbor – ebgp-multihop** – Enables BGP to establish connection with external peers

- **neighbor – next-hop-self** – Enables BGP to send itself as the next hop for advertised routes
- **neighbor – interval** – Configures neighbor interval
- **neighbor – timers** – Configures neighbor KeepAlive Time and Hold Time Intervals
- **neighbor – shutdown** – Disables the Peer session
- **neighbor – update-source** - Configures the source-address for routing updates and for TCP connection establishment with a peer
- **neighbor – gateway** - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer

Chapter 46

ISIS

The list of CLI commands for the configuration of ISIS is as follows:

- router isis
- net
- route-leak
- ls-type
- summary-address
- ipra <ipra-idx>
- ipra <ipra-index>
- set-overload-bit
- area-password
- domain-password
- nsf ietf
- nsf t1 interval
- nsf t2
- nsf t3 manual
- nsf ietf restart-reason

- nsf ietf helper-support
- nsf ietf helper gracetimelimit
- distribute-list route-map
- distance
- ip router isis
- isis ipv6 addr
- isis circuit-type
- isis metric
- isis hello-interval
- isis hello-multiplier
- isis password
- isis lsp
- isis retransmit-interval
- isis priority
- debug isis
- isis csnp-interval
- show ip isis instances
- show ip isis circuits
- show ip isis- adjacencies
- show ip isis- routes
- show ipv6 - routes
- show ip isis - interface-info
- show ip isis - debug-info
- show ip isis - packet-stats
- show isis nsf

46.1 router isis

This command creates the ISIS routing process for providing Connectionless Mode Network Service of ISIS module. The no form of this command disables the ISIS routing process.

```
router isis [vrf <contextname>]

no router isis [vrf <contextname>]
```

Syntax Description	**vrf <contextname>**	-	Enables ISIS module for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
Mode	Global configuration Mode		
Package	Enterprise and Metro		
Default	disable		
Example	`iss(config)# router isis vrf xyz`		

Related Commands

- **net –** Configures Network entity title for the system
- **route-leak –** Enable Route Leak Feature
- **is-type –** Configures the system type for an instance of ISIS router
- **summary-address –** Configures a summary address for an instance
- **ipra <ipra-index> –** Configures the IP Reachability address for an instance
- **ipra<ipra-index> –** Configures the metric for IP Reachability address for an instance
- **set-overload-bit –** Sets the overload bit
- **area-password –** Configures the area authentication password for an instance
- **domain-password –** Configures the routing domain authentication password for an instance
- **nsf ietf –** Enable graceful restart mechanism in router
- **nsf t1 interval –** Configures the number of times the restarting router will resend the restart TLV with RR bit set
- **nsf t1 retry-count –** Configures the amount of time , in seconds that the restarting router waits for L1/L2 database sync-up
- **nsf t2 –** Configures the amount of time , in seconds that the restarting router waits for L1/L2 database sync-up

	• **nsf t3 manual –** Configures the amount of time , in seconds that the restarting router waits before setting overload bit • **nsf ietf restart-reason –** Enables helper support for restarting router only or both restarting and starting router (router not having capability to preserve forwarding plane • **nsf ietf helper gracetimelimit –** Configures the helper grace time limit • **distribute-list route-map –** Enable route map filtering for inbound or outbound routes • **distance –** Disables the distance. • **ip router isis –** Enables ISIS on an interface • **isis ipv6 addr –** Configures the IP Reachability address for an instance • **isis circuit-type –** Configure the circuit type • **isis metric –** Configures the metric for the given level • **isis hello-interval –** Configures the hello-interval for the given level • **isis hello-multiplier –** Configures the hello-multiplier for the given level • **isis password –** Configures the password for authenticating Hello PDUs • **isis lsp –** Configures the lsp interval • **isis retransmit-interval –** Configures the retransmit interval for point to point circuits. • **isis priority –** Configures the priority for the given level • **debug isis –** Enables the debug for the given module • **isis csnp-interval –** Configure the csnp interval for the given level as 10 • **show ip isis instances** - Displays the information about the instances of isis • **show ip isis circuits** - Displays the information about the circuits of isis • **show ip isis adjacencies** - Displays the information about the adjacencies existing on the given interface • **show ip isis routes –** Displays the routing table for the given instance and level • **show ip isis database –** Displays the lsp database for the given level • **show ipv6 isis –** Displays the routing table for the given instance and level • **show ip isis interface-info –** Displays the level specific interface information • **show ip isis debug-info –** Displays the modules whose debug is enabled • **show ip isis packet-stats –** Displays the packet statistics for the given interface • **show isis nsf -** Display Graceful restart status

46.2 net

This command configures the network entity title for the system and the manual area address for the ISIS router. The no form of the command deletes the manual area address for the router

net <network-entity-title>

no net <network-entity-title>

Syntax Description	**<network-entity-title>**	-	Configures the manual area address for the ISIS router
Mode	ISIS Mode		
Package	Enterprise and Metro		
Default	00:00:00:00:00:00:00:00		
Example	`iss(config-router)# net 01:02:00:00:00:00:00:00`		

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.
- **ip router isis –** Enables ISIS on an interface
- **show ip isis instances** - Displays the information about the instances of isis
- **show ip isis circuits –** Displays the Displays information about the circuits of isis

46.3 route-leak

This command enables the route leak feature and allows the Level 2 router to leak in to Level 1 router, through specially tagged routes which will not be re-advertised into Level 2 router. The no form of the command disables the route leak feature.

route-leak

no route-leak

Mode ISIS Mode

Package Enterprise and Metro

Default Disable

Example

```
iss(config-router)# route-leak
```

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis -** Enables ISIS router.

46.4 is-type

This command configures the ISIS router type as Level 1 or Level 2. The no form of the command configures the system type for an instance as Level12 ISIS router.

is-type {level-1 | level1-2 | level-2-only}

no is-type

Syntax Description

level-1	-	Configures the router as Intra-area routers which exchange information between Level 1 routers and other Level 1 router.
Level1-2	-	Configures the router as Inter area routers which exchange information with Level 1 and Level 2 routers and connects intra area and inter area routers.
level-2-only		Configures the router as inter area routers which exchange information only with Level 2 routers.

Mode ISIS Mode

Default Level 1-2

Package Enterprise and Metro

Example

```
iss(config-router)# is-type level-1
```

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.
- **show ip isis instances** - Displays the information about the instances of isis
- **show ip isis circuits –** Displays the Displays information about the circuits of isis

46.5 summary-address

This command configures the summary address which aggregates the addresses that are represented in the routing table; routes from other routing protocols can also be summarized. One summary address can include multiple groups of addresses for a given level. The no form of the command deletes the summary address.

```
summary-address {<address> <mask> | <ip6_addr> <prefixlength>}{level-1 |
level1-2 | level-2-only}

no summary-address {<address> <mask> | <ip6_addr> <prefixlength>}
```

Syntax Description

<address>	-	Configures the summary address for the designated range of addresses
<mask>	-	Configures the subnet mask for the IP address. This is a 32-bit number which is used to divide the IP address into network address and host address.
<ip6_addr>	-	Configures the IPv6 address
<prefixlength>	-	Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network.
level-1	-	Configures the summary address for the Level 1 router
level1-2	-	Configures the summary address for the Level 1 - 2 router
level-2-only	-	Configures the summary address for the Level 2 only router

Mode ISIS Mode

Package Enterprise and Metro

Example

```
onfig-router)# summary-address 12.0.0.1 255.0.0.0 level-1
```

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.

46.6 ipra <ipra-idx>

This command configures the IP reachable address with its next hop information.

```
ipra <ipra-idx> {<ip-address> <ip-mask> <next-hop-ip> | <ip6_addr>
<prefixlength> <ip6_addr> } [met-type {internal | external}]
```

Syntax Description	**<ipra-idx>**	-	Configures the circuit level ipra index. The ipra index ranges between (1-2000000000).
	<ip-address>	-	Configure the destination IPv4 address.
	<ip-mask>		Configures the subnet mask for the IP address. This is a 32-bit number which is used to divide the IP address into network address and host address.
	<next-hop-ip>		Configures the next hop destination IPv4 address.
	<ip6_addr>		Configure the destination IPv6 address.
	<prefixlength>		Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network.
	<ip6_addr>		Configures the next hop destination IPv6 address.
	met-type		Configures the type of the Metric as internal or external metric ranges from 1-63
	internal		Configures the metric type as internal, which means that the metric of the route will compete with all other internal routes.
	external		Configures the metric as external metric, which means the external metric is considered as less desirable than internal metric
Mode	ISIS Mode		
Default	Internal		
Package	Enterprise and Metro		
Example	`#iss(config-router)# ipra 64 12.0.0.1 255.0.0.0 12.0.0.2`		
☞	This command is executed only if the router isis is enabled		

Related commands

- **`router isis –`** Enables ISIS router.
- **`show ipv6 isis-routes -`** Displays the ipv6 routing table for the given instance and level
- **`show ip isis- routes -`** Displays the routing table for the given instance and level of the routers.

46.7 ipra <ipra-index>

This command configures the type of metric for IP reachability address for the ISIS router. The no form of the command configures the IP reachability address for the instance.

```
ipra <ipra-index> default-metric <metric> [delay-metric <metric>] [error-
metric <metric>] [expense-metric <metric>]

no ipra <ipra-idx>
```

Syntax Description

<ipra-index>	Configures the circuit level ipra index. The ipra index ranges between 1 and 2000000000.
default-metric <metric>	Configures default metric value of this IP reachability address. The value ranges between 0 and 63.
delay-metric <metric>	Configures the delay metric value of this IP reachability address. The value ranges between 0 and 63.
error-metric <metric>	Configures the error metric value of this IP reachability address. The value ranges between 0 and 63.
expense-metric <metric>	Configures the expense metric value of this IP reachability address. The value ranges between 0 and 63.

Mode ISIS Mode

Package Enterprise and Metro

Example

```
#iss(config-router)#  ipra 64 default-metric 55 32
```

This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.
- **show ipv6 isis-routes -** Displays the ipv6 routing table for the given instance and level
- **show ip isis- routes -** Displays the routing table for the given instance and level of the routers.

46.8 set-overload-bit

This command configures the router to set the overload bit in its non-pseudo node LSPs. The setting of overload bit is allowed only when Link State database is not complete, resulting in an incomplete / inaccurate routing table. By setting the overload bit in its LSPs, other routers can ignore the unreliable router in their SPF calculations until the router has recovered from its problems and no paths through this router are seen by other routers in the IS-IS area. The no form of the command resets the overload bit

`set-over load-bit`

`no set-overload-bit`

Mode	ISIS Mode
Package	Enterprise
Default	Overload clear
Example	`#iss(config-router)# set-overload-bit`
☞	This command is executed only if the router isis is enabled
Related commands	**`router isis -`** Enables ISIS router

46.9 area-password

This command configures the area authentication password for an instance. This password is used for authentication of Level 1 control PDUs during transmission and reception. The password size is 0 and 16. The no form of the command removes the area authentication password.

area-password <password>

no area-password <password>

Mode	ISIS Mode
Package	Enterprise and Metro
Example	`#iss(config-router)# area-password xyz15`
☞	This command is executed only if the router isis is enabled
Related commands	• **router isis –** Enables ISIS router.

46.10 domain-password

This command configures the routing domain authentication password for an instance. This password is used for authentication of Level 2 control PDUs during transmission and reception. The password size is 0 and 16. The no form of the command removes the routing domain password

domain-password <password>

no domain-password <password>

Mode ISIS Mode

Package Enterprise and Metro

Example
```
iss(config-router)# domain-password xyz15
```
☞ This command is executed only if the router isis is enabled

Related commands **router isis –** Enables ISIS router.

46.11 nsf ietf

This command enables graceful restart mechanism in router which allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a processor switch over. When graceful restart is enabled, peer networking devices are informed, through protocol extensions prior to the event. The graceful restart mechanism is implemented in ISIS module based on Internet Engineering Task forwarding standard. The no form of the command

`nsf ietf {plannedOnly | plannedAndUnplanned}`

`no nsf ietf`

Syntax Description	**`plannedOnly`**	-	Configures planned only graceful restart mechanism in the router
	`plannedAndUnplanned`	-	Configures both planned and unplanned graceful restart mechanism in the router
Mode	ISIS Mode		
Package	Enterprise and Metro		
Default	none		
Example	`#iss(config-router)# nsf ietf plannedOnly`		
☞	This command is executed only if the router isis is enabled		
Related commands	• **`router isis –`** Enables ISIS router.		
	• **`show isis nsf -`** Displays Graceful restart status		

46.12 nsf t1 interval

This command configures T1 time-interval which defines the maximum time for sending Hellos with Grace TLVs on each interface of a restarting router. The T1 time-interval is the maximum time for reception of graceful restart acknowledgment and CNSPs from a Helping/Running the router. The time interval value ranges from 1 to 180. The no form of the command configures the time interval for sending hello packets with RR-bit to default t1 interval

nsf t1 interval

no nsf t1 interval

Mode ISIS Mode

Default 3

Package Enterprise and Metro

Example

```
#iss(config-router)# nsf t1 interval 40
```

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.
- **show isis nsf -** Displays Graceful restart status.

46.13 nsf t1 retry-count

This command describes the number of times the restarting router will resend the Graceful Restart TLV with RR bit set. The Grace TLV is sent till Grace Acks, CSNPs are received from DIS routers. The no form of the command resets the T1 retry count to default T1 retry count.

```
nsf t1 retry-count <count>

no nsf t1 retry-count
```

Syntax Description	`<count>`	-	Configures the retry count value of the router. The value ranges between 1 to 200
Mode	ISIS Mode		
Default	1		
Package	Enterprise and Metro		
Example	`#iss(config-isis)# nsf t1 retry-count 50`		
☞	This command is executed only if the router isis is enabled		
Related commands	• **`router isis`** – Enables ISIS router. • **`show isis nsf`** - Displays Graceful restart status.		

46.14 nsf t2

This command configures T2 time interval in seconds which defines the maximum wait time for the synchronization of the Level 1 / Level 2 LSDB on a restarting/starting router. The no form of the command resets the t2 time to default value for that level

```
nsf t2 {level-1 | level1-2 | level-2 }  <seconds>

no nsf t2 level-2 {level-1 | level1-2 | level-2 }
```

Syntax Description

level-1	-	Configures T2 interval for Level 1 routers
level1-2	-	Configures T2 interval for Level 1-2
level-2	-	Configures T2 interval for level-2 routers
<seconds>	-	Configures T2 time interval in seconds. The value ranges between 1-32767

Mode ISIS Mode

Default 60

Package Enterprise and Metro

Example

```
#iss(config-router)# nsf t2 level-1 44
```

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.
- **show isis nsf -** Displays Graceful restart status.

46.15 nsf t3 manual

This command configures amount of time, for supporting graceful restart on a Restarting router. The value ranges from 1and 65535. The no form of the command resets the t3 time interval to default value.

nsf t3 manual <seconds>

no nsf t3 manual

Mode Configure Mode

Default 120

Package Enterprise and Metro

Example

```
#iss(config-router)# nsf t3 manual 55
```

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.
- **show isis nsf -** Displays Graceful restart status

46.16 nsf ietf restart-reason

This command configures the reason for the graceful restart of the ISIS router. The reason for restart can be software upgrade, scheduled restart or switch to redundant router.

nsf ietf restart-reason
[{unknown|softwareRestart|swReloadUpgrade|switchToRedundant}]

Syntax Description	**unknown**	-	Configures the system to restarts due to unplanned events (such as restarting after a crash).
	softwareRestart	-	Configures the system to restart due to restart of software.
	swReloadUpgrade	-	Configures the system to restart due to reload or upgrade of software.
	switchToRedundant	-	Configures the system to restart due to switchover to a redundant support processor.

Mode ISIS Mode

Default Unknown

Example
```
#iss(config-router)# nsf ietf restart-reason softwareRestart
```

Package Enterprise and Metro

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.
- **show isis nsf -** Displays Graceful restart status.

46.17 nsf ietf helper-support

The command enables helper policy for neighboring ISIS Routers undergoing graceful restart that is the helper support is enabled only for restarting router or for both restarting and starting router. The no form of the command disables the helper support.

nsf ietf helper-support [{restart|both}]

no nsf ietf helper-support

Syntax Description

restart	- Configures helper support only for the restarting router that ensures forwarding plane preservation.
both	- Configures helper support for both the restarting and starting routers that support/donot support forwarding plane preservation.

Mode ISIS Mode

Default No helper support

Package Enterprise and Metro

Example

```
#iss(config-router)# nsf ietf helper-support restart
```

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.
- **show isis nsf -** Displays Graceful restart status.

46.18 nsf ietf helper gracetimelimit

This command configures the grace period till which the router acts as helper. During this period, the router advertises that the restarting router is active and is in FULL state. The value ranges between 1 and 1800 seconds. The value is provided as an intimation of the restart period to the neighbors that do not support graceful restart or that are connected using multipoint interfaces. The no form of the command configures the helper grace time limit as zero.

nsf ietf helper gracetimelimit <gracelimit>

no nsf ietf helper gracetimelimit

Mode ISIS Mode

Default 180

Package Enterprise and Metro

Example

```
iss(config-router)# nsf ietf helper gracetimelimit 190
```

☞ This command is executed only if the router isis is enabled

Related commands

- **router isis –** Enables ISIS router.
- **show isis nsf -** Displays Graceful restart status.

46.19 distribute-list route-map

This command enables route map filtering for inbound or outbound routes and defines the conditions for distributing the routes from one routing protocol to another. The no form of the command disables inbound filtering for the routes.

```
distribute-list route-map <name(1-20)> {in }

no distribute-list route-map <name(1-20)> { in }
```

Syntax Description	`route-map <name(1-20)>`	-	Configures the name of the Route Map for which filtering should be enabled. This value is a string of size 20.
	`in`	-	Configures filtering for in bound routers
Mode	ISIS Mode		
Package	Enterprise and Metro		
Example	`iss(config-router)# distribute-list route-map rmap in`		

☞

- This command is executed only if the router isis is enabled
- This command will be available only if the "**Router wanted** "switch is given as **YES** while building exe file.

Related commands

- **`router isis`** – Enables ISIS router.
- **`distance`** – Disables the distance.

46.20 distance

This command enables the administrative distance that is the metric to reach destination of the routing protocol and sets the administrative distance value. The distance value ranges between 1 and 255. This distance value will not be used for distribute list. The administrative distance can be enabled for only one route map. The distance should be disabled for the already assigned route map, if distance needs to be enabled for another route map. The no form of the command disables the administrative distance.

```
distance <1-255> [route-map <name(1-20)>]

no distance [route-map <name(1-20)>]
```

Syntax Description

`<1-255>`	-	Configures the distance. The value rangers between 1 and 255.
`route-map <name(1-20)>`	-	Configures the name of the Route Map for which filtering should be enabled. This value is a string of size 20.

Mode ISIS Mode

Package Enterprise and Metro

Example

```
iss(config-isis)# distance 10 route-map rmap
```

☞

- This command is executed only if the router isis is enabled
- This command will be available only if the "**Router wanted** "switch is given as **YES** while building exe file.

Related commands

- **`router isis`** – Enables ISIS router.
- **`distribute-list route-map`** – Enables route map filtering for inbound or outbound routes

46.21 ip router isis

This command configures IS-IS routing process for IPv6 on an interface and attaches an area designator to the routing process. The no form of the command disables the ISIS router on an interface

ip router isis

no ip router isis

Mode Interface configuration mode (Vlan Interface Mode)

Default Disable

Package Enterprise and Metro

Example

```
iss(config-if)# ip router isis
```

- This command is executed only if the **router isis** is enabled
- Network entity title must be assigned before executing this command

Related commands

- **router isis –** Enables ISIS router.
- **net** – Configures an IS-IS network entity title for the routing process.
- **isis circuit-type –** Configures the circuit type which defines the type of adjacency desired for neighbors.
- **isis ipv6 addr –** Configures the IP Reachability address for an instance
- **isis circuit-type –** Configure the circuit type
- **isis metric –** Configures the metric for the given level
- **isis hello-interval –** Configures the hello-interval for the given level
- **isis hello-multiplier –** Configures the hello-multiplier for the given level
- **isis password –** Configures the password for authenticating Hello PDUs
- **isis lsp –** Configures the lsp interval
- **isis retransmit-interval –** Configures the retransmit interval for point to point circuits.
- **isis priority –** Configures the priority for the given level
- **debug isis –** Enables the debug for the given module
- **isis csnp-interval –** Configure the csnp interval for the given level as 10
- **show ip isis instances** - Displays the information about the instances of isis
- **show ip isis circuits** - Displays the information about the circuits of isis
- **show ip isis adjacencies** - Displays the information about the adjacencies existing on the given interface
- **show ip isis routes –** Displays the routing table for the given instance and level
- **show ip isis database –** Displays the lsp database for the given level
- **show ipv6 isis –** Displays the routing table for the given instance and level
- **show ip isis interface-info –** Displays the level specific interface information
- **show ip isis debug-info –** Displays the modules whose debug is enabled
- **show ip isis packet-stats –** Displays the packet statistics for the given interface
- **show isis nsf -** Display Graceful restart status

46.22 isis ipv6 addr

This command configures the Link-local IPv6 address of the neighbor in the ISIS router. The no form of the command disables the configuration of the IPv6 address.

isis ipv6 addr <ip6_addr> <prefixlength>

no isis ipv6 addr <ip6_addr> <prefixlength>

Syntax Description

ipv6 addr <ip6_addr>	-	Configures the IPv6 address of the neighbor in the ISIS router.
<prefixlength>	-	Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network

Mode Interface configuration mode (Vlan Interface Mode)

Package Enterprise and Metro

Example `iss(config-if)# isis ipv6 addr fe80::211:11ff:fe56:3dcb 64`

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled

Related commands

- **router isis –** Enables ISIS router.
- **ip router isis** IS-IS routing process for IPv6 on an interface

46.23 isis circuit-type

This command configures the circuit type which defines the type of adjacency desired for neighbors on the specified interface. The no form of the command configures the circuit type as level 1-2

```
isis circuit-type {level-1 | level1-2 | level-2-only}

no isis circuit-type
```

Syntax Description

level-1	-	Configures Level 1 adjacency, if there is at least one area address in common between this system and its neighbors.
level1-2	-	Configures Level 2 adjacencies, if the other routers are Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies will never be established over this interface
level-2-only	-	Configures Level 1 and Level 2, if the neighbor is also configured as level-1-2 and there is at least one area in common

Mode Interface configuration mode (Vlan Interface Mode)

Default Level 2

Package Enterprise and Metro

Example

```
iss(config-if)# isis circuit-type level-1
```

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled

Related commands

- **router isis –** Enables ISIS router.
- **ip router isis –** IS-IS routing process for IPv6 on an interface
- **show ip isis circuits** - Displays the information about the circuits of isis

46.24 isis metric

This command is assigned to link and used to calculate the cost for sending a packet from each other router through the links on an interface in a network to other destinations. The no form of the command sets the default metric value for the interface.

```
isis metric <default-metric> [delay-metric <metric>] [error-metric <metric>]
[expense-metric <metric>] {level-1 | level-2}

no isis metric {level-1 | level-2}
```

Syntax Description

delay-metric <metric>	- Configures delay metric value of this IP reachability address. The delay metric value ranges between 0 and 63.
error-metric <metric>	- Configures the error metric value of this IP reachability address. The error metric value ranges between 0 and 63.
expense-metric <metric>	- Configures the expense metric value of this IP reachability address. The expense metric value ranges between 0 and 63.
level-1	- Configures the metric value for Level 1 routers
level-2	- Configures the metric value for Level 2 routers

Mode Interface configuration mode (Vlan Interface Mode)

Package Enterprise and Metro

Default

metric	-	20
Level	-	Level1-2

Example

```
iss(config-if)# isis metric 35 level-1
```

☞

Related commands

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled
- **router isis –** Enables ISIS router.
- **ip router isis** IS-IS routing process for IPv6 on an interface
- **show ipv6 isis-routes -** Displays the ipv6 routing table for the given instance and level
- **show ip isis routes -** Displays the routing table for the given instance and level of the routers.

46.25 isis hello-interval

This command specifies the length of the time (in seconds, ranges between 1-60) between hello packets sent on the interface. The no form of the command sets default value for, interval between hello packets sent on the interface.

```
isis hello-interval <interval> {level-1 | level-2}

no isis hello-interval {level-1 | level-2}
```

Syntax Description

level-1	-	Configures the hello interval for level-1 routers.
level-2	-	Configures the hello interval for level-2 routers

Mode Interface configuration mode (Vlan Interface Mode)

Package Enterprise and Metro

Default

Hello interval	-	10
Level	-	Level 1-2

Example

```
iss(config-if)#  isis hello-interval 12 level-1
```

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled

Related commands

- **router isis –** Enables ISIS router.
- **ip router isis** IS-IS routing process for IPv6 on an interface
- **isis hello-multiplier** – Configures the hello-multiplier for the routers

46.26 isis hello-multiplier

This command configures the hello-multiplier for the given level, which specifies the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency as down. This value is multiplied by the corresponding Hello Timer and used as the holding time in transmitted hellos. Using a smaller hello-multiplier will give fast convergence, but can result in more routing instability hence increment the hello-multiplier to a larger value to increase the network stability.
The value ranges between 2 and 100.

```
isis hello-multiplier <hello-interval> {level-1 | level-2}

no isis hello-multiplier {level-1 | level-2}
```

Syntax Description

level-1	-	Configures the hello multiplier for Level 1 router
level-2	-	Configures the hello multiplier for Level 2 routers

Mode Interface configuration mode (Vlan Interface Mode)

Package Enterprise and Metro

Default

Hello interval	-	10
Level	-	Level 2

Example

```
iss(config-if)# isis hello-multiplier 15 level-1
```

☞

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled

Related commands

- **router isis –** Enables ISIS router.
- **hello-interval -** Configures the hello interval for a router on a interface
- **ip router isis** IS-IS routing process for IPv6 on an interface

46.27 isis password

This command configures the authentication password for Level 1 or Level 2 routers, respectively based on the specified Levels and enables to prevent (string size max of 16) unauthorized routers from forming adjacencies with this router. The no form of the command disables the authentication for the routers.

```
isis password <password> {level-1 | level-2}

no isis password <password> {level-1 | level-2}
```

Syntax Description

level-1	-	Configures the authentication password for Level 1 router
level-2	-	Configures the authentication password for Level 2 router

Mode Interface configuration mode (Vlan Interface Mode)

Package Enterprise and Metro

Default

Level	-	Level 1
Authentication	-	Disable

Example

```
iss(config-if)# isis password j123 level-1
```

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled

Related commands

- **router isis –** Enables ISIS router.
- **ip router isis** IS-IS routing process for IPv6 on an interface.

46.28 isis lsp

This command configures the delay between successive IS-IS link state packet transmissions range which allows the LSP transmission rate to be reduced. The value ranges between 1 and 65535. The no form of the command restores the default value.

isis lsp-interval <interval>

no isis lsp-interval

Mode Interface configuration mode (Vlan Interface Mode)

Default 900seconds

Package Enterprise and Metro

Example

```
iss(config-if)# isis lsp-interval 100
```

Related Commands

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled
- **router isis –** Enables ISIS router.
- **isis retransmit-interval** – Configures the number of seconds between retransmission of IS-IS link
- **ip router isis** IS-IS routing process for IPv6 on an interface
- **show ip isis – database -** Displays the lsp database for the given level of the ISIS routers.

46.29 isis retransmit-interval

This command configure the number of seconds between retransmission of IS-IS link state PDUs (LSPs) on a point-to-point links. The value ranges between 1 to 300. The no form of the command configures the retransmission interval to default value.

isis retransmit-interval <interval>

no isis retransmit-interval

Mode Interface configuration mode (Vlan Interface Mode)

Default 5 seconds

Package Enterprise and Metro

Example

```
iss(config-if)# isis retransmit-interval 60
```

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled

Related Commands

- **router isis –** Enables ISIS router.
- **isis lsp interval –** Configures the delay between successive IS-IS link state packet transmissions
- **ip router isis –** IS-IS routing process for IPv6 on an interface

46.30 isis priority

This command configures the priorities for Level 1 and Level 2, which is used for designated router election. These priority values are advertised in the hellos and are used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The router with the highest priority will become the DIS. The value ranges between 0 to 127. The no form of the command configures the default priority value.

```
isis priority <priority> {level-1 | level-2}

no isis priority {level-1 | level-2}
```

Syntax Description

level-1	-	Configures the priority value for Level 1 routers
level-2	-	Configures the priority value for Level 2 routers

Mode Interface configuration mode (Vlan Interface Mode)

Default

Priority value	-	64
level	-	Level 1-2

Package Enterprise and Metro

Example

```
iss(config-if)# isis priority 80 level-1
```

Related Commands

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled
- **router isis –** Enables ISIS router.
- **hello-interval -** Configures the hello interval for a router on a interface
- **ip router isis –** IS-IS routing process for IPv6 on an interface

46.31 debug isis

This command enables the debug of the isis module and configures the various debug and trace statements to handle error and event management available in the isis module. The traces are enabled by passing the necessary parameters. The no form of the command resets debug options for ISIS module.

```
debug isis [vrf <contextname>] {adjn | decn | updt | all}

no debug isis [vrf <contextname>] {adjn | decn | updt | all}
```

Syntax Description

vrf <contextname>	-	This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
adjn	-	Generates traces for adjacency related information
decn	-	Generates traces for SPF decisions
updt	-	Generates traces for isis updates
all	-	Generates all types of trace messages

Mode Privilege Execution Mode

Default Tracing of the ISIS module is disabled

Package Enterprise and Metro

Example

```
iss# debug isis default all
```

Related Command

- **show ip isis debug-info –** Displays the module whose debug is enable

46.32 isis csnp-interval

This command configures the Complete sequence number PDUs (CSNPs) interval for a level, which is sent by the designated router to maintain database synchronization. The no form of the command configures the CNSP interval as default value.

```
isis csnp-interval <interval> {level-1 | level-2}

no isis csnp-interval <interval> {level-1 | level-2}
```

Syntax Description

level-1	-	Configures the interval of time between transmission of CSNPs for Level 1
level-2	-	Configures the interval of time between transmission of CSNPs for Level 2

Mode Interface configuration mode (Vlan Interface Mode)

Package Enterprise and Metro

Default

CNSP interval	-	10 seconds
Level	-	Level1-2

Example

```
iss(config-if)# isis csnp-interval 30 level-1
```

- This command is executed only if the **router isis** is enabled
- This command is executed only if the **ip router isis** is enabled

Related Commands

- **router isis –** Enables ISIS router.
- **ip router isis –** IS-IS routing process for IPv6 on an interface

46.33 show ip isis instances

This command displays the information about the instances of ISIS routers. The information contains system Index, System ID, System type and Operating state. The operating state of the system will be up once the network entity title is configured.

show ip isis instances

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip isis instances

SystemIdx   System-ID          SysType     OperState

-----------------------------------------------------

0           00:00:00:00:00:00   OTHER       DOWN
```

☞ This command is executed only if the **ip router isis** is enabled

Related commands

- **router isis –** Enables ISIS router.
- **is-type –** Configures the system type for an instance of ISIS router
- **net –** Configures Network entity title for the system
- **ip router isis –** IS-IS routing process for IPv6 on an interface

46.34 show ip isis circuits

This command displays the Displays information about the circuits of ISIS. The information contains circuit index, Instance index, circuit type, level and operating state. The operating state of the system will be up once the network entity title is configured.

show ip isis circuits

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip isis circuits

CktIdx     InstIdx    IfIdx      CktType    Level      OperState
-------------------------------------------------------------
1          0          33         BCAST      LEVEL12    DOWN
```

☞ This command is executed only if the **ip router isis** is enabled

Related commands

- **isis circuit-type –** Configures the circuit type for the instance
- **is-type –** Configures the system type for an instance of ISIS router
- **net –** Configures Network entity title for the system
- **ip router isis –** IS-IS routing process for IPv6 on an interface

46.35 show ip isis- adjacencies

This command displays the information about the adjacencies existing on the given interface.

```
show ip isis [vrf <contextname> adjacencies [ { vlan <integer(1-4094)> |
<iftype> <ifnum> }]
```

Syntax Description

`vrf <contextname>`	-	Enables ISIS module for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
`adjacencies`	-	Displays the adjacencies which are defined as the neighbors over a single circuit where ISIS is enabled. Adjacency can be either an end system or intermediate system
`vlan <integer(1-4094)>`	-	Displays the ISIS for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094
`<iftype>`	-	Displays the interface specific ISIS related information for the specified type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
`<ifnum>`	-	Displays the interface specific ISIS related information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1.

Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip isis adjacencies

      DIS information
        ----------------
       LAN DIS Id          :00:00:00:00:00:03

       LEVEL1 Adjacency
         ----------------
       AdjSysId          :00:00:00:00:00:03
       Adjacency State IS: UP
       Adjacency Usage IS: LEVEL1
       IPV4 Address IS   : 28:00:00:03
```

☞ This command is executed only if the **ip router isis** is enabled

Related commands

- **ip router isis –** IS-IS routing process for IPv6 on an interface
- **router isis -** Enables ISIS router.

46.36 show ip isis- routes

This command displays the routing table for the given instance and level of the routers. The information contains destination ID, Metric value, metric type and the Next hop address.

show ip isis [vrf <contextname>] routes {level-1 | level-2}

Syntax Description

vrf <contextname>	-	Enables ISIS module for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
routes	-	Displays the routing table for Level 1 and Level 2 routers
level-1	-	Displays the routing table for Level 1 routers
level-2	-	Displays the routing table for Level 2 routers

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip isis routes level-1
Dest ID          Metric       MetType         Next Hop
-------------------------------------------------------
40.00.00.00          10      DEFAULT_MET     LOCAL
20.00.00.00          10      DEFAULT_MET     LOCAL
```

☞ This command is executed only if the **ip router isis** is enabled

Related commands

- **ip router isis –** IS-IS routing process for IPv6 on an interface
- **isis metric –** Calculates the cost for sending a packet from each other router through the links.
- **ipra <ipra-index> –** Configures the type of metric for IP reachability address for the ISIS router
- **ipra <ipra-idx> –** Configures the IP reachable address with its next hop information

46.37 show ip isis- database

This command displays the lsp database for the given level of the ISIS routers. This information contains LSP-ID, LSP sequence number, LSP checksum and LSP Hold time.

show ip isis [vrf <contextname>] database [{level-1 | level-2 }] [detailed] [lspid <id>]

Syntax Description	**vrf <contextname>**	-	Enables ISIS module for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
	database	-	Displays the LSP database information of the ISIS
	level-1	-	Displays the information of the LSP database for level-1 routers
	level-2	-	Displays the information of the LSP database for level-2 routers
	detailed	-	Displays the detailed LSP database information of the ISIS
	lspid <id>	-	Displays the LSP id which is an identifier for the Link State information of the intermediate system in a given area. LSP is used to calculate the shortest path from this IS to all IS in the area.

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip isis database level-1
ISIS : Level 1 LSP Database
LSP-ID    LSP Seq Num   LSP Checksum  LSP Hold time  P/ATT/OL
ISIS : Level 1 LSP Database
LSP-ID   LSP Seq Num   LSP Checksum  LSP Hold time  P/ATT/OL
00:00:00:00:00:02:00:00  00000001       2109   1200   0/0/0
00:00:00:00:00:02:00:01  00000001       3a67   1200   0/0/0
00:00:00:00:00:03:00:00  00000001       1910   1042   0/0/0
```

```
00:00:00:00:00:03:00:01   00000001        2e0c    1042    0/0/0

00:00:00:00:00:03:02:00   00000002        dd39    1042    0/0/0

00:00:00:00:00:03:02:01   00000002        1eb5    1042    0/0/0
```

☞ This command is executed only if the **ip router isis** is enabled

Related commands

- **`ip router isis –`** IS-IS routing process for IPv6 on an interface
- **`isis lsp`** - Configures the delay between successive IS-IS link state packet transmissions range

46.38 show ipv6 - routes

This command displays the ipv6 routing table for the given instance and level. This information contains destination ID, Metric value, metric type and the Next hop address.

show ipv6 isis [vrf <contextname>] routes {level-1 | level-2 }

Syntax Description

vrf <contextname>	-	Enables ISIS module for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
routes	-	Displays the ipv6 routing table for level 1 and level 2 routers
level-1	-	Displays the ipv6 routing table for level 1 routers
level-2	-	Displays the ipv6 routing table for level 2 routers

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip isis routes level-1

Dest ID             Metric  MetType        NextHop
-------------------------------------------------------------
40.00.00.00         10      DEFAULT_MET    LOCAL
20.00.00.00         10      DEFAULT_MET    LOCAL
```

This command is executed only if the **ip router isis** is enabled

Related commands

- **ip router isis –** IS-IS routing process for IPv6 on an interface
- **isis metric –** Calculates the cost for sending a packet from each other router through the links.
- **ipra <ipra-index> –** Configures the type of metric for IP reachability address for the ISIS router
- **ipra <ipra-idx> –** Configures the IP reachable address with its next hop information

46.39 show ip isis - interface-info

This command displays the level specific interface information

```
show ip isis [vrf <contextname>] interface-info [ { vlan <integer(1-4094)> |
<iftype> <ifnum> }] {level-1 | level-2 }
```

Syntax Description

`vrf <contextname>`	-	Enables ISIS module for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
`interface-info`	-	Displays the interface-info which defines the Ethernet interface on which the ISIS protocol is enabled
`vlan <integer(1-4094)`	-	Displays the ISIS for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094
`<iftype>`		Displays the interface specific ISIS related information for the specified type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
`<ifnum>`		Displays the interface specific ISIS related information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1.

Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip isis interface-info level-1
```

Metric	Priority	Hello Interval	Hello Multiplier	LSP Interval	LSP-Retransmit Interval	CSNP Interval
10	64	3000	10	10	5	10

☞ This command is executed only if the **ip router isis** is enabled

Related commands **`ip router isis –`** IS-IS routing process for IPv6 on an interface

46.40 show ip isis - debug-info

This command displays the modules whose debug is enabled

```
show ip isis [vrf <contextname>] debug-info
```

Syntax Description	`vrf <contextname>`	-	Enables ISIS module for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
	`debug-info`		Displays the debug info which contains informational messages on receive, update and forwarding process of ISIS protocol over a single circuit.

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip isis debug-info
```

☞ This command is executed only if the **ip router isis** is enabled

Related commands

- **`debug isis`** – Enables the debug of the ISIS module.
- **`ip router isis`** – IS-IS routing process for IPv6 on an interface

46.41 show ip isis - packet-stats

This command displays the packet statistics for the specified interface

```
show ip isis [vrf <contextname>] packet-stats [ { vlan <integer(1-4094)> |
<iftype> <ifnum> }]
```

Syntax Description

`vrf <contextname>`	-	Enables ISIS module for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
`packet-stats`	-	Displays the packet-stats information which provides the count of number of ISIS packets (ISIS Hello, LSPDU, CSNP, PSNP) received and transmitted over an interface where the ISIS is enabled
`vlan <integer(1-4094)`	-	Displays the ISIS for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094
`iftype`	-	Displays the interface specific ISIS related information for the specified type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
`ifnum`	-	Displays the interface specific ISIS related information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is

0 and port number is 1.

Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip isis packet-stats

Received Packet Statistics for LEVEL1

Hello PDUs:                        205
Link State PDUs:                   4
Complete SeqNo PDUs:               20
Partial SeqNo PDU:                 0

Sent Packet Statistics for LEVEL1

Hello PDUs:                          94
Link State PDUs:                     2
Complete SeqNo PDUs:                 0
Partial SeqNo PDU:                   0
```

☞ This command is executed only if the **ip router isis** is enabled

Related commands

- **ip router isis –** IS-IS routing process for IPv6 on an interface

46.42 show isis nsf

This command displays the status of the graceful restart. The information contains T1 interval, T2 interval, T3 interval, Restart Mode, Restart status, Helper support and grace time limit.

show isis nsf

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show isis nsf

Restart Support :
    Non-Stop Forwarding disabled
T1 Timer Interval limit: 3
T2 Timer Interval limit for Level1: 60
T2 Timer Interval limit for Level2: 60
Restart-interval(T3) limit: 120
T1 Timer Retry Count: 1
Restart Mode :
    Acting as Normal Router
Restart Status :
    Non-Stop Forwarding disabled
Last NSF restart:
    No Restart Happened
Restart Reason is:
    Unknown
Helper Support:
    No Helper Support
Helper Grace Time Limit: 180
Graceful Restart State:ISIS_GR_NORMAL_ROUTER
```

Related commands

- **nsf ietf –** Enables graceful restart
- **nsf t1 interval -** Configures T1 time-interval for the routers
- **nsf t1 retry-count -** Describes the number of times the restarting router will resend the Graceful Restart TLV with RR bit set.
- **nsf t2 -** Configures T2 time interval for the routers
- **nsf t3 manual -** Defines the maximum time for supporting graceful restart
- **nsf ietf restart-reason -** Configures the reason for the graceful restart
- **nsf ietf helper support** - Enables helper policy for neighboring ISIS Routers
- **nsf ietf helper gracetime** - Configures the grace period till which the router acts as helper