

ipx nlsip enable

To enable NetWare Link-Services Protocol (NLSP) routing on the primary network configured on this interface or subinterface, use the **ipx nlsip enable** command in interface configuration mode. To disable NLSP routing on the primary network configured on this interface or subinterface, use the **no** form of this command.

ipx nlsip [tag] enable

no ipx nlsip [tag] enable

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
---------------------------	------------	--

Defaults	NLSP is disabled on all interfaces.
-----------------	-------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines When you enable NLSP routing, the current settings for RIP and SAP compatibility modes as specified with the **ipx nlsip rip** and **ipx nlsip sap** interface configuration commands take effect automatically.

When you specify an NLSP *tag*, the router enables NLSP on the specified process. An NLSP *process* is a router's databases working together to manage route information about an area. NLSP version 1.0 routers are always in the same area. Each router has its own adjacencies, link-state, and forwarding databases. These databases operate collectively as a single *process* to discover, select, and maintain route information about the area. NLSP version 1.1 routers that exist within a single area also use a single process.

NLSP version 1.1 routers that interconnect multiple areas use multiple processes to discover, select, and maintain route information about the areas they interconnect. These routers manage an adjacencies, link-state, and area address database for each area to which they attach. Collectively, these databases are still referred to as a *process*. The forwarding database is shared among processes within a router. The sharing of entries in the forwarding database is automatic when all processes interconnect NLSP version 1.1 areas.

Configure multiple NLSP processes when a router interconnects multiple NLSP areas.



Note

NLSP version 1.1 routers refer to routers that support the route aggregation feature, while NLSP version 1.0 routers refer to routers that do not.

Examples	The following example enables NLSP routing on Ethernet interface 0:
-----------------	---

```
interface ethernet 0
 ipx nlspace enable
```

The following example enables NLSP routing on serial interface 0:

```
interface serial 0
 ipx ipxwan 2442 unnumbered local1
 ipx nlspace enable
```

The following example enables NLSP routing for process area3 on Ethernet interface 0:

```
interface ethernet 0
 ipx nlspace area3 enable
```

Related Commands

Command	Description
ipx nlspace rip	Configures RIP compatibility when NLSP is enabled.
ipx nlspace sap	Configures SAP compatibility when NLSP is enabled.

ipx nlsip hello-interval

To configure the interval between the transmission of hello packets, use the **ipx nlsip hello-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx nlsip [*tag*] **hello-interval** *seconds*

no ipx nlsip [*tag*] **hello-interval** *seconds*

Syntax Description		
<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.	
<i>seconds</i>	Time, in seconds, between the transmission of hello packets on the interface. It can be a number in the range 1 to 1600. The default is 10 seconds for the designated router and 20 seconds for nondesignated routers.	

Defaults	
	10 seconds for the designated router. 20 seconds for nondesignated routers.

Command Modes	
	Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	
	The designated router sends hello packets at an interval equal to one-half the configured value.
	Use this command to improve the speed at which a failed router or link is detected. A router is declared to be down if a hello has not been received from it for the time determined by the holding time (the hello interval multiplied by the holding time multiplier; by default, 60 seconds for nondesignated routers and 30 seconds for designated routers). You can reduce this time by lowering the hello-interval setting, at the cost of increased traffic overhead.
	You may also use this command to reduce link overhead on very slow links by raising the hello interval. This will reduce the traffic on the link at the cost of increasing the time required to detect a failed router or link.

Examples	
	The following example configures serial interface 0 to transmit hello packets every 30 seconds:

```
interface serial 0
 ipx ipxwan 2442 unnumbered local1
 ipx nlsip enable
 ipx nlsip hello-interval 30
```

Related Commands

Command	Description
ipx nlsnp csnp-interval	Configures the NLSP CSNP interval.
ipx nlsnp hello-multiplier	Configures the time delay between successive NLSP LSP transmissions.
ipx nlsnp retransmit-interval	Configures RIP compatibility when NLSP is enabled.

ipx nlsip hello-multiplier

To specify the hello multiplier used on an interface, use the **ipx nlsip hello-multiplier** command in interface configuration mode. To restore the default value, use the **no** form of this command.

```
ipx nlsip [tag] hello-multiplier multiplier
```

```
no ipx nlsip [tag] hello-multiplier
```

Syntax Description		
<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.	
<i>multiplier</i>	Value by which to multiply the hello interval. It can be a number in the range 3 to 1000. The default is 3.	

Defaults The default multiplier is 3.

Command Modes Interface configuration

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines You use the hello modifier in conjunction with the hello interval to determine the holding time value sent in a hello packet. The holding time is equal to the hello interval multiplied by the hello multiplier.

The holding time tells the neighboring router how long to wait for another hello packet from the sending router. If the neighboring router does not receive another hello packet in the specified time, then the neighboring router declares that the sending router is down.

You can use this method of determining the holding time when hello packets are lost with some frequency and NLSP adjacencies are failing unnecessarily. You raise the hello multiplier and lower the hello interval correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.

Examples In the following example, serial interface 0 will advertise hello packets every 15 seconds. The multiplier is 5. These values determine that the hello packet holding time is 75 seconds.

```
interface serial 0
 ipx nlsip hello-interval 15
 ipx nlsip hello-multiplier 5
```

Related Commands	Command	Description
	ipx nlsip hello-interval	Specifies the hello multiplier used on an interface.

ipx nlsplsp-interval

To configure the time delay between successive NetWare Link-Services Protocol (NLSP) link-state packet (LSP) transmissions, use the **ipx nlsplsp-interval** command in interface configuration mode. To restore the default time delay, use the **no** form of this command.

ipx nlspltag] lsp-interval interval

no ipx nlspltag] lsp-interval

Syntax Description

<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
<i>interval</i>	Time, in milliseconds, between successive LSP transmissions. The interval can be a number in the range 55 and 5000. The default interval is 55 milliseconds (ms).

Defaults

55 milliseconds

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command allows you to control how fast LSPs can be flooded out an interface.

In topologies with a large number of NLSP neighbors and interfaces, a router may have difficulty with the CPU load imposed by LSP transmission and reception. This command allows you to reduce the LSP transmission rate (and by implication the reception rate of other systems).

Examples

The following example causes the system to transmit LSPs every 100 ms (10 packets per second) on Ethernet interface 0:

```
interface Ethernet 0
 ipx nlsplsp-interval 100
```

Related Commands

Command	Description
ipx nlspretransmit-interval	Configures RIP compatibility when NLSP is enabled.

ipx nlspl metric

To configure the NetWare Link-Services Protocol (NLSP) cost for an interface, use the **ipx nlspl metric** command in interface configuration mode. To restore the default cost, use the **no** form of this command.

ipx nlspl [*tag*] **metric** *metric-number*

no ipx nlspl [*tag*] **metric** *metric-number*

Syntax Description	
<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
<i>metric-number</i>	Metric value for the interface. It can be a number from 0 to 63.

Defaults The default varies on the basis of the throughput of the link connected to the interface.

Command Modes Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines Use the **ipx nlspl metric** command to cause NLSP to prefer some links over others. A link with a lower metric is more preferable than one with a higher metric.

Typically, it is not necessary to configure the metric; however, it may be desirable in some cases when there are wide differences in link bandwidths. For example, using the default metrics, a single 64-kbps ISDN link will be preferable to two 1544-kbps T1 links.

Examples The following example configures a metric of 10 on serial interface 0:

```
interface serial 0
 ipx network 107
 ipx nlspl enable
 ipx nlspl metric 10
```

Related Commands	Command	Description
	ipx nlspl enable	Configures the interval between the transmission of hello packets.

ipx nlsf multicast

To configure an interface to use multicast addressing, use the **ipx nlsf multicast** command in interface configuration mode. To configure the interface to use broadcast addressing, use the **no** form of this command.

ipx nlsf [*tag*] **multicast**

no ipx nlsf [*tag*] **multicast**

Syntax Description

tag (Optional) Names the NLSP process. The tag can be any combination of printable characters.

Defaults

Multicast addressing is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command allows the router interface to use NLSP multicast addressing. If an adjacent neighbor does not support NLSP multicast addressing, the router will revert to using broadcasts on the affected interface.

The router will also revert to using broadcasts if multicast addressing is not supported by the hardware or driver.

Examples

The following example disables multicast addressing on Ethernet interface 0:

```
interface ethernet 0
  no ipx nlsf multicast
```

ipx nlsppriority

To configure the election priority of the specified interface for designated router election, use the **ipx nlsppriority** command in interface configuration mode. To restore the default priority, use the **no** form of this command.

ipx nlsppriority [*tag*] **priority** *priority-number*

no ipx nlsppriority [*tag*] **priority** *priority-number*

Syntax Description		
<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.	
<i>priority-number</i>	Election priority of the designated router for the specified interface. This can be a number in the range 0 to 127. This value is unitless. The default is 44.	

Defaults 44

Command Modes Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines Use the **ipx nlsppriority** command to control which router is elected designated router. The device with the highest priority number is selected as the designated router.

The designated router increases its own priority by 20 in order to keep its state as of the designated router more stable. To have a particular router be selected as the designated router, configure its priority to be at least 65.

Examples The following example sets the designated router election priority to 65:

```
interface ethernet 0
 ipx network 101
 ipx nlsppriority enable
 ipx nlsppriority 65
```

ipx nlsr retransmit-interval

To configure the link-state packet (LSP) retransmission interval on WAN links, use the **ipx nlsr retransmit-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx nlsr [*tag*] **retransmit-interval** *seconds*

no ipx nlsr [*tag*] **retransmit-interval** *seconds*

Syntax Description

<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
<i>seconds</i>	LSP retransmission interval, in seconds. This can be a number in the range 1 to 30. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command sets the maximum amount of time that can pass before an LSP will be sent again (retransmitted) on a WAN link, if no acknowledgment is received.

Reducing the retransmission interval can improve the convergence rate of the network in the face of lost WAN links. The cost of reducing the retransmission interval is the potential increase in link utilization.

Examples

The following example configures the LSP retransmission interval to 2 seconds:

```
ipx nlsr retransmit-interval 2
```

Related Commands

Command	Description
ipx nlsr csnp-interval	Configures the NLSP CSNP interval.
ipx nlsr hello-interval	Specifies the hello multiplier used on an interface.

ipx nlsip rip

To configure RIP compatibility when NetWare Link-Services Protocol (NLSP) is enabled, use the **ipx nlsip rip** command in interface configuration mode. To restore the default, use the **no** form of this command.

```
ipx nlsip [tag] rip [on | off | auto]
```

```
no ipx nlsip [tag] rip [on | off | auto]
```

Syntax Description	
<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
on	(Optional) Always generates and sends RIP periodic traffic.
off	(Optional) Never generates and sends RIP periodic traffic.
auto	(Optional) Sends RIP periodic traffic only if another RIP router in sending periodic RIP traffic. This is the default.

Defaults RIP periodic traffic is sent only if another router in sending periodic RIP traffic.

Command Modes Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines The **ipx nlsip rip** command is meaningful only on networks on which NLSP is enabled. (RIP and SAP are always on by default on other interfaces.) Because the default mode is **auto**, no action is normally required to fully support RIP compatibility on an NLSP network.

Examples In the following example, the interface never generates or sends RIP periodic traffic:

```
interface ethernet 0
 ipx nlsip rip off
```

Related Commands	Command	Description
	ipx nlsip enable	Configures the interval between the transmission of hello packets.
	ipx nlsip sap	Configures SAP compatibility when NLSP in enabled.

ipx nlsap

To configure SAP compatibility when NetWare Link-Services Protocol (NLSP) is enabled, use the **ipx nlsap sap** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipx nlsap [*tag*] **sap** [**on** | **off** | **auto**]

no ipx nlsap [*tag*] **sap** [**on** | **off** | **auto**]

Syntax Description

<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
on	(Optional) Always generates and sends SAP periodic traffic.
off	(Optional) Never generates and sends SAP periodic traffic.
auto	(Optional) Sends SAP periodic traffic only if another SAP router is sending periodic SAP traffic. This is the default.

Defaults

SAP periodic traffic is sent only if another router is sending periodic SAP traffic.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **ipx nlsap sap** command is meaningful only on networks on which NLSP is enabled. Because the default mode is **auto**, no action is normally required to fully support SAP compatibility on an NLSP network.

Examples

In the following example, the interface never generates or sends SAP periodic traffic:

```
interface ethernet 0
 ipx nlsap sap off
```

Related Commands

Command	Description
ipx nlsap enable	Configures the interval between the transmission of hello packets.
ipx nlsap rip	Configures RIP compatibility when NLSP is enabled.

ipx output-ggs-filter

To control which servers are included in the Get General Service (GGS) responses sent by Cisco IOS software, use the **ipx output-ggs-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

```
ipx output-ggs-filter {access-list-number | name}
```

```
no ipx output-ggs-filter {access-list-number | name}
```

Syntax Description

<i>access-list-number</i>	Number of the Service Advertising Protocol (SAP) access list. All outgoing GGS packets are filtered by the entries in this list. The <i>access-list number</i> is a number from 1000 to 1099.
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent their being confused with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

You can issue only one **ipx output-ggs-filter** command on each interface.



Note

Because GGS SAP response filters are applied ahead of output SAP filters, a SAP entry permitted to pass through the GGS SAP response filter can still be filtered by the output SAP filter.

Examples

The following example excludes the server at address 3c.0800.89a1.1527 from GGS responses sent on Ethernet interface 0, but allows all other servers:

```
access-list 1000 deny 3c.0800.89a1.1527
access-list 1000 permit -1
ipx routing

interface ethernet 0
 ipx network 2B
 ipx output-ggs-filter 1000
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx output-gns-filter	Controls which servers are included in the GGS responses sent by the Cisco IOS software.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx router-sap-filter	Filters SAP messages received from a particular router.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx output-gns-filter

To control which servers are included in the Get Nearest Server (GNS) responses sent by Cisco IOS software, use the **ipx output-gns-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

```
ipx output-gns-filter {access-list-number | name}
```

```
no ipx output-gns-filter {access-list-number | name}
```

Syntax Description

<i>access-list-number</i>	Number of the SAP access list. All outgoing GNS packets are filtered by the entries in this access list. The argument <i>access-list-number</i> is a number from 1000 to 1099.
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can issue only one **ipx output-gns-filter** command on each interface.

Examples

The following example excludes the server at address 3c.0800.89a1.1527 from GNS responses sent on Ethernet interface 0, but allows all other servers:

```
access-list 1000 deny 3c.0800.89a1.1527
access-list 1000 permit -1
ipx routing

interface ethernet 0
 ipx network 2B
 ipx output-gns-filter 1000
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx gns-round-robin	Rotates using a round-robin selection method through a set of eligible servers when responding to GNS requests.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx output-network-filter (RIP)

To control the list of networks included in routing updates sent out an interface, use the **ipx output-network-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

```
ipx output-network-filter {access-list-number | name}
```

```
no ipx output-network-filter {access-list-number | name}
```

Syntax Description

<i>access-list-number</i>	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, <i>access-list-number</i> is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx output-network-filter** command controls which networks the Cisco IOS software advertises in its IPX routing updates (RIP updates).

You can issue only one **ipx output-network-filter** command on each interface.

Examples

In the following example, access list 896 controls which networks are specified in routing updates sent out the serial 1 interface. This configuration causes network 2b to be the only network advertised in Novell routing updates sent on the specified serial interface.

```
access-list 896 permit 2b

interface serial 1
 ipx output-network-filter 896
```

Related Commands	Command	Description
	access-list (IPX extended)	Defines an extended Novell IPX access list.
	access-list (IPX standard)	Defines a standard IPX access list.
	deny (extended)	Sets conditions for a named IPX extended access list.
	deny (standard)	Sets conditions for a named IPX access list.
	ipx access-list	Defines an IPX access list by name.
	ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
	ipx router-filter	Filters the routers from which packets are accepted.
	permit (IPX extended)	Sets conditions for a named IPX extended access list.
	pre-interval	Sets conditions for a named IPX access list.

ipx output-rip-delay

To set the interpacket delay for RIP updates sent on a single interface, use the **ipx output-rip-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipx output-rip-delay *delay*

no ipx output-rip-delay [*delay*]

Syntax Description	<i>delay</i>	Delay, in milliseconds (ms), between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.
---------------------------	--------------	---

Defaults	55 ms
-----------------	-------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. The **ipx output-rip-delay** command sets the interpacket delay for a single interface.

The system uses the interpacket delay specified by the **ipx output-rip-delay** command for periodic and triggered routing updates when no delay is set for triggered routing updates. When you set a delay for triggered routing updates, the system uses the delay specified by the **ipx output-rip-delay** command for only the periodic routing updates sent on the interface.

To set a delay for triggered routing updates, see the **ipx triggered-rip-delay** or **ipx default-triggered-rip-delay** commands.

You can also set a default RIP interpacket delay for all interfaces. See the **ipx default-output-rip-delay** command for more information.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX machines. These machines may lose RIP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX machines.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Examples

The following example establishes a 55-ms interpacket delay on serial interface 0:

```
interface serial 0
```

```
ipx network 106A
ipx output-rip-delay 55
```

Related Commands

Command	Description
ipx default-output-rip-delay	Sets the default interpacket delay for RIP updates sent on all interfaces
ipx default-triggered-rip-delay	Sets the default interpacket delay for triggered RIP updates sent on all interfaces.
ipx triggered-rip-delay	Sets the interpacket delay for triggered RIP updates sent on a single interface.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx output-sap-delay

To set the interpacket delay for Service Advertising Protocol (SAP) updates sent on a single interface, use the **ipx output-sap-delay** command in interface configuration mode. To return to the default delay value, use the **no** form of this command.

ipx output-sap-delay *delay*

no ipx output-sap-delay

Syntax Description	<i>delay</i>	Delay, in milliseconds, between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.
---------------------------	--------------	--

Defaults	55 ms
-----------------	-------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The interpacket delay is the delay between the individual packets sent in a multiple-packet SAP update. The **ipx output-sap-delay** command sets the interpacket delay for a single interface.

The system uses the interpacket delay specified by the **ipx output-sap-delay** command for periodic and triggered SAP updates when no delay is set for triggered updates. When you set a delay for triggered updates, the system uses the delay specified by the **ipx output-sap-delay** command only for the periodic updates sent on the interface.

To set a delay for triggered updates, see the **ipx triggered-sap-delay** or **ipx default-triggered-sap-delay** commands.

You can also set a default SAP interpacket delay for all interfaces. See the **ipx default-output-sap-delay** command for more information.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by the **ipx output-sap-delay** command forces the router to pace its output to the slower-processing needs of these servers.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Examples The following example establishes a 55-ms delay between packets in multiple-packet SAP updates on Ethernet interface 0:

```
interface ethernet 0
 ipx network 106A
 ipx output-sap-delay 55
```

Related Commands

Command	Description
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx default-triggered-sap-delay	Sets the default interpacket delay for triggered SAP updates sent on all interfaces.
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx triggered-sap-delay	Sets the interpacket delay for triggered SAP updates sent on a single interface.

ipx output-sap-filter

To control which services are included in Service Advertising Protocol (SAP) updates sent by Cisco IOS software, use the **ipx output-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

```
ipx output-sap-filter {access-list-number | name}
```

```
no ipx output-sap-filter {access-list-number | name}
```

Syntax Description	
<i>access-list-number</i>	Number of the SAP access list. All outgoing service advertisements are filtered by the entries in this access list. The argument <i>access-list-number</i> is a number from 1000 to 1099.
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults No filters are predefined.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Cisco IOS software applies output SAP filters prior to sending SAP packets. You can issue only one **ipx output-sap-filter** command on each interface. When configuring SAP filters for NetWare 3.11 and later servers, use the server's internal network and node number (the node number is always 0000.0000.0001) as its address in the SAP **access-list** command. Do not use the *network.node* address of the particular interface board.

Examples The following example denies service advertisements about server 0000.0000.0001 on network aa from being sent on network 4d (via Ethernet interface 1). All other services are advertised via this network. All services, included those from server aa.0000.0000.0001, are advertised via networks 3c and 2b.

```
access-list 1000 deny aa.0000.0000.0001
access-list 1000 permit -1

interface ethernet 0
 ipx network 3c

interface ethernet 1
 ipx network 4d
 ipx output-sap-filter 1000
```

```
interface serial 0
 ipx network 2b
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx gns-round-robin	Rotates using a round-robin selection method through a set of eligible servers when responding to GNS requests.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx router-sap-filter	Filters SAP messages received from a particular router.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx pad-process-switched-packets

To control whether odd-length packets are padded so as to be sent as even-length packets on an interface, use the **ipx pad-process-switched-packets** command in interface configuration mode. To disable padding, use the **no** form of this command.

ipx pad-process-switched-packets

no ipx pad-process-switched-packets

Syntax Description This command has no arguments or keywords.

Defaults Enabled on Ethernet interfaces.
Disabled on Token Ring, FDDI, and serial interfaces.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Use this command only under the guidance of a customer engineer or other service representative.

The **ipx pad-process-switched-packets** command affects process-switched packets only, so you must disable fast switching before the **ipx pad-process-switched-packets** command has any effect.

Some IPX end hosts reject Ethernet packets that are not padded. Certain topologies can result in such packets being forwarded onto a remote Ethernet network. Under specific conditions, padding on intermediate media can be used as a temporary workaround for this problem.

Examples The following example configures the Cisco IOS software to pad odd-length packets so that they are sent as even-length packets on FDDI interface 1.

```
interface fddi 1
 ipx network 2A
 no ipx route-cache
 ipx pad-process-switched-packets
```

Related Commands	Command	Description
	ipx route-cache	Enables IPX fast switching.

ipx per-host-load-share

To enable per-host load sharing, use the **ipx per-host-load-share** command in global configuration mode. To disable per-host load sharing, use the **no** form of this command.

ipx per-host-load-share

no ipx per-host-load-share

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines Use this command to enable per-host load sharing. Per-host load sharing transmits traffic across multiple, equal-cost paths while guaranteeing that packets for a given end host always take the same path.

When you do not enable per-host load sharing, the software uses a round-robin algorithm to accomplish load sharing. Round-robin load sharing transmits successive packets over alternate, equal-cost paths, regardless of the destination host. With round-robin load sharing, successive packets destined for the same end host might take different paths. Thus, round-robin load sharing increases the possibility that successive packets to a given end host might arrive out of order or be dropped, but ensures true load balancing of a given workload across multiple links.

In contrast, per-host load sharing decreases the possibility that successive packets to a given end host will arrive out of order; but, there is a potential decrease in true load balancing across multiple links. True load sharing occurs only when different end hosts utilize different paths; equal link utilization cannot be guaranteed.

With per-host load balancing, the number of equal-cost paths set by the **ipx maximum-paths** command must be greater than one; otherwise, per-host load sharing has no effect.

Examples The following command globally enables per-host load sharing:

```
ipx per-host-load share
```

Related Commands	Command	Description
	ipx maximum-paths	Sets the maximum number of equal-cost paths the Cisco IOS software uses when forwarding packets.

ipx ping-default

To select the ping type that Cisco IOS software transmits, use the **ipx ping-default** command in global configuration mode. To return to the default ping type, use the **no** form of this command.

```
ipx ping-default { cisco | novell | diagnostic }
```

```
no ipx ping-default { cisco | novell | diagnostic }
```

Syntax Description		
	cisco	Transmits Cisco pings.
	novell	Transmits standard Novell pings.
	diagnostic	Transmits diagnostic request/response for IPX pings.

Defaults Cisco pings

Command Modes Global configuration

Command History	Release	Modification
	10.3	This command was introduced.
	12.0	The diagnostic keyword was added.

Usage Guidelines This command can transmit Cisco pings, standard Novell pings as defined in the NLSP specification, and IPX diagnostic pings.

The IPX diagnostic ping feature addresses diagnostic related issues by accepting and processing unicast or broadcast diagnostic packets. It makes enhancements to the current IPX ping command to ping other stations using the diagnostic packets and display the configuration information in the response packet.



Note

When a ping is sent from one station to another, the response is expected to come back immediately; when **ipx ping-default** is set to diagnostics, the response could consist of more than one packet and each node is expected to respond within 0.5 seconds of receipt of the request. Due to the absence of an end-of-message flag, there is a delay and the requester must wait for all responses to arrive. Therefore, in verbose mode there may be a brief delay of 0.5 seconds before the response data is displayed.

The **ipx ping-default** command using the **diagnostic** keyword can be used to conduct a reachability test and should not be used to measure accurate roundtrip delay.

Examples The following is sample output from the **ipx ping-default** command when the **diagnostic** keyword is enabled:

```
Router# ipx ping-default diagnostic
```

```

Protocol [ip]: ipx
Target IPX address: 20.0000.0000.0001
Verbose [n]: y
Timeout in seconds [2]: 1
Type escape sequence to abort.
Sending 1, 31-byte IPX Diagnostic Echoes to 20.0000.0000.0001, timeout is 1 seconds:

Diagnostic Response from 20.0000.0000.0001 in 4 ms
Major Version: 1
Minor Version: 0
SPX Diagnostic Socket: 4002
Number of components: 3
Component ID: 0 (IPX / SPX)
Component ID: 1 (Router Driver)
Component ID: 5 (Router)
Number of Local Networks: 2
  Local Network Type: 0 (LAN Board)
    Network Address1 20
    Node Address1 0000.0000.0001
  Local Network Type: 0 (LAN Board)
    Network Address2 30
    Node Address2 0060.70cc.bc65
    
```



Note Verbose mode must be enabled to get diagnostic information.

Related Commands

Command	Description
ping (privileged)	Diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks.
trace (privileged)	Discovers the specified protocol's routes that packets will actually take when traveling to their destination.

ipx potential-pseudonode (NLSP)

To enable NetWare Link Services Protocol (NLSP) to keep backup router and service information for potential pseudonode, use the **ipx potential-pseudonode** command in global configuration mode. To disable the feature so that NLSP does not keep backup router and service information for potential pseudonode, use the **no** form of this command.

ipx potential-pseudonode

no ipx potential-pseudonode

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines The potential pseudonode is NLSP-specified service information that a router keeps in anticipation of possibly becoming a designated router. Designated routers are required to produce an actual pseudonode.

Examples The following example enables NLSP to keep backup router and service information for potential pseudonode:

```
ipx potential-pseudonode
```

ipx rip-max-packetsize

To configure the maximum packet size of RIP updates sent out the interface, use the **ipx rip-max-packetsize** command in interface configuration mode. To restore the default packet size, use the **no** form of this command.

ipx rip-max-packetsize *bytes*

no ipx rip-max-packetsize *bytes*

Syntax Description	<i>bytes</i>	Maximum packet size in bytes. The default is 432 bytes, which allows for 50 routes at 8 bytes each, plus 32 bytes of IPX network and RIP header information.
---------------------------	--------------	--

Defaults	432 bytes
-----------------	-----------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	The maximum size is for the IPX packet including the IPX network and RIP header information. Do not allow the maximum packet size to exceed the allowed maximum size of packets for the interface.
-------------------------	---

Examples	The following example sets the maximum RIP update packet to 832 bytes: <pre>ipx rip-max-packetsize 832</pre>
-----------------	---

Related Commands	Command	Description
	ipx sap-max-packetsize	Configures the maximum packet size of SAP updates sent out the interface.

ipx rip-multiplier

To configure the interval at which a network's RIP entry ages out, use the **ipx rip-multiplier** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx rip-multiplier *multiplier*

no ipx rip-multiplier *multiplier*

Syntax Description	<i>multiplier</i>	Multiplier used to calculate the interval at which to age out RIP routing table entries. This can be any positive number. The value you specify is multiplied by the RIP update interval to determine the aging-out interval. The default is three times the RIP update interval.
---------------------------	-------------------	---

Defaults	Three times the RIP update interval
-----------------	-------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	All routers on the same physical cable should use the same multiplier value.
-------------------------	--

Examples In the following example, in a configuration where RIP updates are sent once every 2 minutes, the interval at which RIP entries age out is set to 10 minutes:

```
interface ethernet 0
 ipx rip-multiplier 5
```

Related Commands	Command	Description
	ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx rip-queue-maximum

To set an IPX Routing Information Protocol (RIP) queue maximum to control how many RIP packets can be waiting to be processed at any given time, use the **ipx rip-queue-maximum** command in global configuration mode. To clear a set RIP queue maximum, use the **no** form of this command.

ipx rip-queue-maximum *milliseconds*

no ipx rip-queue-maximum *milliseconds*

Syntax Description	<i>milliseconds</i>	Specifies the queue limit as a number from 0 to the maximum unassigned integer.
---------------------------	---------------------	---

Defaults	No queue limit is set.
-----------------	------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	When you use the ipx rip-queue-maximum command to control how many RIP packets can be waiting to be processed at any given time, remember that if the queue limit is reached, the incoming RIP request packets are dropped. Be sure to set a large enough queue limit to handle normal incoming RIP requests on all interfaces, or else the RIP information may time out.
-------------------------	--

Examples	The following example sets a RIP queue maximum of 500 milliseconds:
-----------------	---

```
ipx rip-queue-maximum 500
```

Related Commands	Command	Description
	ipx rip-update-queue-maximum	Sets an IPX RIP queue maximum to control how many incoming RIP update packets can be waiting to be processed at any given time.
	ipx sap-queue-maximum	Sets an IPX SAP queue maximum to control how many SAP packets can be waiting to be processed at any given time.
	ipx sap-update-queue-maximum	Sets an IPX SAP queue maximum to control how many incoming SAP update packets can be waiting to be processed at any given time.

ipx rip-update-queue-maximum

To set an IPX Routing Information Protocol (RIP) queue maximum to control how many incoming RIP update packets can be waiting to be processed at any given time, use the **ipx rip-update-queue-maximum** command in global configuration mode. To clear a set RIP queue maximum, use the **no** form of this command.

ipx rip-update-queue-maximum *queue-maximum*

no ipx rip-update-queue-maximum *queue-maximum*

Syntax Description	<i>queue-maximum</i>	Specifies the queue limit as a number from 0 to the maximum unassigned integer.
---------------------------	----------------------	---

Defaults	No queue limit
-----------------	----------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	When you use the ipx rip-update-queue-maximum command to control how many incoming RIP update packets can be waiting to be processed at any given time, remember that if the queue limit is reached, the incoming RIP update packets are dropped.
-------------------------	--



Note	When using the ipx rip-update-queue-maximum command, be sure to set this queue high enough to handle a full update on all interfaces, or else the RIP information may time out.
-------------	--

Examples	The following example sets a RIP update queue maximum of 500: <pre>ipx rip-update-queue-maximum 500</pre>
-----------------	--

Related Commands	Command	Description
	ipx rip-queue-maximum	Sets an IPX RIP queue maximum to control how many RIP packets can be waiting to be processed at any given time.
	ipx sap-queue-maximum	Sets an IPX SAP queue maximum to control how many SAP packets can be waiting to be processed at any given time.
	ipx sap-update-queue-maximum	Sets an IPX SAP queue maximum to control how many incoming SAP update packets can be waiting to be processed at any given time.

ipx rip-response-delay

To change the delay when responding to Routing Information Protocol (RIP) requests, use the **ipx rip-response-delay** command in interface configuration mode. To return to the default delay, use the **no** form of this command.

ipx rip-response-delay *ms*

no ipx rip-response-delay

Syntax Description

<i>ms</i>	Delay time, in milliseconds, for RIP responses.
-----------	---

Defaults

No delay in answering (0 ms).

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command slows down the Cisco router and allows another router to answer first and become the router of choice. A delay in responding to RIP requests can be imposed so that, in certain topologies, any local Novell IPX router or any third-party IPX router can respond to the RIP requests before the Cisco router responds.

Optimal delay time is the same as or slightly longer than the time it takes the other router to answer.

Examples

The following example sets the delay in responding to RIP requests to 55 ms (0.055 seconds):

```
ipx rip-response-delay 55
```

Related Commands

Command	Description
ipx gns-response-delay	Changes the delay when responding to GNS requests.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.

ipx route

To add a static route or static NetWare Link Services Protocol (NLSP) route summary to the routing table, use the **ipx route** command in global configuration mode. To remove a route from the routing table, use the **no** form of this command.

```
ipx route {network [network-mask] | default} {network.node | interface} [ticks] [hops]
[floating-static]
```

```
no ipx route
```

Syntax Description	
<i>network</i>	<p>Network to which you want to establish a static route.</p> <p>This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.</p>
<i>network-mask</i>	<p>(Optional) Specifies the portion of the network address that is common to all addresses in an NLSP route summary. When used with the <i>network</i> argument, it specifies the static route summary.</p> <p>The high-order bits of <i>network-mask</i> must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted.</p>
default	<p>Creates a static entry for the “default route.” The router forwards all nonlocal packets for which no explicit route is known via the specified next hop address (<i>network.node</i>) or interface.</p>
<i>network.node</i>	<p>Router to which to forward packets destined for the specified network.</p> <p>The argument <i>network</i> is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.</p> <p>The argument <i>node</i> is the node number of the target router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxx.xxx</i>).</p>
<i>interface</i>	<p>Network interface to which to forward packets destined for the specified network. Interface is serial 0 or serial 0.2. Specifying an interface instead of a network node is intended for use on IPXWAN unnumbered interfaces. The specified interface can be a null interface.</p>
<i>ticks</i>	<p>(Optional) Number of IBM clock ticks of delay to the network for which you are establishing a static route. One clock tick is 1/18 of a second (approximately 55 ms). Valid values are 1 through 65,534.</p>

<i>hops</i>	(Optional) Number of hops to the network for which you are establishing a static route. Valid values are 1 through 254.
floating-static	(Optional) Specifies that this route is a floating static route, which is a static route that can be overridden by a dynamically learned route.

Defaults

No static routes are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following arguments and keywords were added: <ul style="list-style-type: none"> • <i>network-mask</i> • default • <i>interface</i> • floating-static

Usage Guidelines

The **ipx route** command forwards packets destined for the specified network (*network*) via the specified router (*network.node*) or an interface (*interface*) on that network regardless of whether that router is sending dynamic routing information.

Floating static routes are static routes that can be overridden by dynamically learned routes. Floating static routes allow you to switch to another path whenever routing information for a destination is lost. One application of floating static routes is to provide back-up routes in topologies where dial-on-demand routing is used.

If you configure a floating static route, the Cisco IOS software checks to see if an entry for the route already exists in its routing table. If a dynamic route already exists, the floating static route is placed in reserve as part of a floating static route table. When the software detects that the dynamic route is no longer available, it replaces the dynamic route with the floating static route for that destination. If the route is later relearned dynamically, the dynamic route replaces the floating static route and the floating static route is again placed in reserve.

If you specify an interface instead of a network node address, the interface must be an IPXWAN unnumbered interface. For IPXWAN interfaces, the network number need not be preassigned; instead, the nodes may negotiate the network number dynamically.

Note that by default, floating static routes are not redistributed into other dynamic protocols.

Examples

In the following example, a router at address 3abc.0000.0c00.1ac9 handles all traffic destined for network 5e:

```
ipx routing
ipx route 5e 3abc.0000.0c00.1ac9
```

The following example defines a static NLSP route summary:

```
ipx routing  
ipx route aaaa0000 ffff0000
```

Related Commands

Command	Description
ipx default-route	Forwards to the default network all packets for which a route to the destination network is unknown.
show ipx route	Displays the contents of the IPX routing table.

ipx route-cache

To enable IPX fast switching, use the **ipx route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

ipx route-cache

no ipx route-cache

Syntax Description This command has no arguments or keywords.

Defaults Fast switching is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Fast switching allows higher throughput by switching packets using a cache created by previous transit packets. Fast switching is enabled by default on all interfaces that support fast switching, including Token Ring, Frame Relay, PPP, Switched Multimegabit Data Service (SMDS), and ATM.

On ciscoBus-2 interface cards, fast switching is done between all encapsulation types. On other interface cards, fast switching is done in all cases *except* the following: transfer of packets with sap encapsulation from an Ethernet, a Token Ring, or an FDDI network to a standard serial line.

You might want to disable fast switching in two situations. One is if you want to save memory on the interface cards: fast-switching caches require more memory than those used for standard switching. The second situation is to avoid congestion on interface cards when a high-bandwidth interface is writing large amounts of information to a low-bandwidth interface.



Note

CiscoBus (Cbus) switching of IPX packets is not supported on the MultiChannel Interface Processor (MIP) interface.

Examples The following example enables fast switching on an interface:

```
interface ethernet 0
 ipx route-cache
```

The following example disables fast switching on an interface:

```
interface ethernet 0
 no ipx route-cache
```

Related Commands	Command	Description
	clear ipx cache	Deletes entries from the IPX fast-switching cache.
	ipx watchdog	Causes the Cisco IOS software to respond to the watchdog packets of a server on behalf of a remote client.
	show ipx cache	Displays the contents of the IPX fast-switching cache.
	show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx route-cache inactivity-timeout

To adjust the period and rate of route cache invalidation because of inactivity, use the **ipx route-cache inactivity-timeout** command in global configuration mode. To return to the default values, use the **no** form of this command.

ipx route-cache inactivity-timeout *period* [*rate*]

no ipx route-cache inactivity-timeout

Syntax Description		
	<i>period</i>	Number of minutes that a valid cache entry may be inactive before it is invalidated. Valid values are 0 through 65,535. A value of zero disables this feature.
	<i>rate</i>	(Optional) Maximum number of inactive entries that may be invalidated per minute. Valid values are 0 through 65,535. A value of zero means no limit.

Defaults The default period is 2 minutes. The default rate is 0 (cache entries do not age).

Command Modes Global configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines IPX fast-switch cache entries that are not in use may be invalidated after a configurable period of time. If no new activity occurs, these entries will be purged from the route cache after one additional minute. Cache entries that have been uploaded to the switch processor when autonomous switching is configured are always exempt from this treatment. This command has no effect if silicon switching is configured.

Examples The following example sets the inactivity period to 5 minutes, and sets a maximum of 10 entries that can be invalidated per minute:

```
ipx route-cache inactivity-timeout 5 10
```

Related Commands	Command	Description
	clear ipx cache	Deletes entries from the IPX fast-switching cache.
	ipx route-cache	Enables IPX fast switching.
	ipx route-cache update-timeout	Adjusts the period and rate of route cache invalidation because of aging.
	show ipx cache	Displays the contents of the IPX fast-switching cache.

ipx route-cache max-size

To set a maximum limit on the number of entries in the IPX route cache, use the **ipx route-cache max-size** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipx route-cache max-size *size*

no ipx route-cache max-size

Syntax Description

<i>size</i>	Maximum number of entries allowed in the IPX route cache.
-------------	---

Defaults

The default setting is no limit on the number of entries.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

On large networks, storing too many entries in the route cache can use a significant amount of router memory, causing router processing to slow. This situation is most common on large networks that run network management applications for NetWare. If the network management station is responsible for managing all clients and servers in a very large (greater than 50,000 nodes) Novell network, the routers on the local segment can become inundated with route cache entries. The **ipx route-cache max-size** command allows you to set a maximum number of entries for the route cache.

If the route cache already has more entries than the specified limit, the extra entries are not deleted. However, all route cache entries are subject to being removed via the parameter set for route cache aging via the **ipx route-cache inactivity-timeout** command.

Examples

The following example sets the maximum route cache size to 10,000 entries.

```
ipx route-cache max-size 10000
```

Related Commands

Command	Description
ipx route-cache	Enables IPX fast switching.
ipx route-cache inactivity-timeout	Adjusts the period and rate of route cache invalidation because of inactivity.
ipx route-cache update-timeout	Adjusts the period and rate of route cache invalidation because of aging.
show ipx cache	Displays the contents of the IPX fast-switching cache.

ipx route-cache update-timeout

To adjust the period and rate of route cache invalidation because of aging, use the **ipx route-cache update-timeout** command in global configuration mode. To return to the default values, use the **no** form of this command.

ipx route-cache update-timeout *period* [*rate*]

no ipx route-cache update-timeout

Syntax Description

<i>period</i>	Number of minutes since a valid cache entry was created before it may be invalidated. A value of zero disables this feature.
<i>rate</i>	(Optional) Maximum number of aged entries that may be invalidated per minute. A value of zero means no limit.

Defaults

The default setting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

IPX fast-switch cache entries that exceed a minimum age may be invalidated after a configurable period of time. Invalidation occurs unless the cache entry was marked as active during the last minute. Following invalidation, if no new activity occurs, these entries will be purged from the route cache after one additional minute.

This capability is primarily useful when autonomous switching or silicon switching is enabled. In both cases, activity is not recorded for entries in the route cache, because data is being switched by the Switch Processor (SP) or Silicon Switch Processor (SSP). In this case, it may be desirable to periodically invalidate a limited number of older cache entries each minute.

If the end hosts have become inactive, the cache entries will be purged after one additional minute. If the end hosts are still active, the route cache and autonomous or SSP cache entries will be revalidated instead of being purged.

Examples

The following example sets the update timeout period to 5 minutes and sets a maximum of 10 entries that can be invalidated per minute:

```
ipx route-cache update-timeout 5 10
```

Related Commands	Command	Description
	clear ipx cache	Deletes entries from the IPX fast-switching cache.
	ipx route-cache	Enables IPX fast switching.
	ipx route-cache inactivity-timeout	Adjusts the period and rate of route cache invalidation because of inactivity.
	show ipx cache	Displays the contents of the IPX fast-switching cache.

ipx router

To specify the routing protocol to use, use the **ipx router** command in global configuration mode. To disable a particular routing protocol on the router, use the **no** form of this command.

ipx router { **eigrp** *autonomous-system-number* | **nlsp** [*tag*] | **rip** }

no ipx router { **eigrp** *autonomous-system-number* | **nlsp** [*tag*] | **rip** }

Syntax Description

eigrp <i>autonomous-system-number</i>	Enables the Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocol. The argument <i>autonomous-system-number</i> is the Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
nlsp [<i>tag</i>]	Enables the NetWare Link Services Protocol (NLSP) routing protocol. The optional argument <i>tag</i> names the NLSP process to which you are assigning the NLSP protocol. If the router has only one process, defining a <i>tag</i> is optional. A maximum of three NLSP processes may be configured on the router at the same time. The <i>tag</i> can be any combination of printable characters.
rip	Enables the Routing Information Protocol (RIP) routing protocol. It is on by default.

Defaults

RIP is enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The following keyword and argument were added: <ul style="list-style-type: none"> • nlsp • <i>tag</i>

Usage Guidelines

You must explicitly disable RIP by issuing the **no ipx router rip** command if you do not want to use this routing protocol.

You can configure multiple Enhanced IGRP processes on a router. To do so, assign each a different autonomous system number.



Note

NLSP version 1.1 routers refer to routers that support the route aggregation feature, while NLSP version 1.0 routers refer to routers that do not.

When you specify an NLSP *tag*, you configure the NLSP routing protocol for a particular NLSP process. An NLSP *process* is a router's databases working together to manage route information about an area. NLSP version 1.0 routers are always in the same area. Each router has its own adjacencies, link-state, and forwarding databases. These databases operate collectively as a single *process* to discover, select, and maintain route information about the area. NLSP version 1.1 routers that exist within a single area also use a single process.

NLSP version 1.1 routers that interconnect multiple areas use multiple processes to discover, select, and maintain route information about the areas they interconnect. These routers manage an adjacencies, link-state, and area address database for each area to which they attach. Collectively, these databases are still referred to as a *process*. The forwarding database is shared among processes within a router. The sharing of entries in the forwarding database is automatic when all processes interconnect NLSP version 1.1 areas.

Configure multiple NLSP processes when a router interconnects multiple NLSP areas.

Examples

The following example enables Enhanced IGRP:

```
ipx router eigrp 4
```

The following example enables NLSP on process area1. This process handles routing for NLSP area 1.

```
ipx router nlspace1
```

Related Commands

Command	Description
network	Enables Enhanced IGRP.
redistribute (IPX)	Redistributes from one routing domain into another.

ipx router-filter

To filter the routers from which packets are accepted, use the **ipx router-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx router-filter { *access-list-number* | *name* }

no ipx router-filter

Syntax Description

<i>access-list-number</i>	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, <i>access-list-number</i> is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can issue only one **ipx router-filter** command on each interface.

Examples

In the following example, access list 866 controls the routers from which packets are accepted. For Ethernet interface 0, only packets from the router at 3c.0000.00c0.047d are accepted. All other packets are implicitly denied.

```
access-list 866 permit 3c.0000.00c0.047d

interface ethernet 0
 ipx router-filter 866
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-list	Defines an IPX access list by name.
ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
ipx output-network-filter (RIP)	Controls the list of networks included in routing updates sent out an interface.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
pre-interval	Sets conditions for a named IPX access list.

ipx router-sap-filter

To filter Service Advertising Protocol (SAP) messages received from a particular router, use the **ipx router-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx router-sap-filter { *access-list-number* | *name* }

no ipx router-sap-filter { *access-list-number* | *name* }

Syntax Description

<i>access-list-number</i>	Number of the access list. All incoming service advertisements are filtered by the entries in this access list. The argument <i>access-list-number</i> is a number from 1000 to 1099.
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can issue only one **ipx router-sap-filter** command on each interface.

Examples

In the following example, the Cisco IOS software will receive service advertisements only from router aa.0207.0104.0874:

```
access-list 1000 permit aa.0207.0104.0874
access-list 1000 deny -1

interface ethernet 0
 ipx router-sap-filter 1000
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx sap	Specifies static SAP entries.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx routing

To enable IPX routing, use the **ipx routing** command in global configuration mode. To disable IPX routing, use the **no** form of this command.

ipx routing [*node*]

no ipx routing

Syntax Description

<i>node</i>	(Optional) Node number of the router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). It must not be a multicast address. If you omit the <i>node</i> argument, the Cisco IOS software uses the hardware MAC address currently assigned to it as its node address. This is the MAC address of the first Ethernet, Token Ring, or FDDI interface card. If no satisfactory interfaces are present in the router (such as only serial interfaces), you must specify a value for the <i>node</i> argument.
-------------	---

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx routing** command enables IPX Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) services.

If you omit the argument *node* and if the MAC address later changes, the IPX node address automatically changes to the new address. However, connectivity may be lost between the time that the MAC address changes and the time that the IPX clients and servers learn the router's new address.

If you plan to use DECnet and IPX routing concurrently on the same interface, you should enable DECnet router first, then enable IPX routing without specifying the optional MAC node number. If you enable IPX before enabling DECnet routing, routing for IPX will be disrupted.

Examples

The following example enables IPX routing:

```
ipx routing
```

Related Commands

Command	Description
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).

ipx sap

To specify static Service Advertising Protocol (SAP) entries, use the **ipx sap** command in global configuration mode. To remove static SAP entries, use the **no** form of this command.

ipx sap *service-type name network.node socket hop-count*

no ipx sap *service-type name network.node socket hop-count*

Syntax Description

<i>service-type</i>	SAP service-type number. See the access-list (SAP filtering) command earlier in this chapter for a table of some IPX SAP services.
<i>name</i>	Name of the server that provides the service.
<i>network.node</i>	Network number and node address of the server. The argument <i>network</i> is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA. The argument <i>node</i> is the node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxx.xxx</i>).
<i>socket</i>	Socket number for this service. See access-list (IPX extended) command earlier in this chapter for a table of some IPX socket numbers.
<i>hop-count</i>	Number of hops to the server.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx sap** command allows you to add static entries into the SAP table. Each entry has a SAP service associated with it. Static SAP assignments always override any identical entries in the SAP table that are learned dynamically, regardless of hop count. The router will not announce a static SAP entry unless it has a route to that network.

Examples

In the following example, the route to JOES_SERVER is not yet learned, so the system displays an informational message. The JOES_SERVER service will not be announced in the regular SAP updates until Cisco IOS software learns the route to it either by means of a RIP update from a neighbor or an **ipx sap** command.

```
ipx sap 107 MAILSERV 160.0000.0c01.2b72 8104 1
ipx sap 4 FILESERV 165.0000.0c01.3d1b 451 1
ipx sap 143 JOES_SERVER A1.0000.0c01.1234 8170 2
no route to A1, JOES_SERVER won't be announced until route is learned
```

Related Commands

Command	Description
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx router-sap-filter	Filters SAP messages received from a particular router.
show ipx servers	Lists the IPX servers discovered through SAP advertisements.

ipx sap follow-route-path

To enable a router to accept IPX Service Advertising Protocol (SAP) entries from SAP updates received on an interface only if that interface is one of the best paths to reach the destination networks of those SAPs, use the **ipx sap follow-route-path** command in global configuration mode. To disable this router function, use **no** form of this command.

ipx sap follow-route-path

no ipx sap follow-route-path

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

In redundantly connected networks that use IPX-Enhanced IGRP routing in which multiple IPX paths exist, IPX SAP services can be learned on nonoptimal interfaces, causing SAP loops, also known as phantom SAPs, when those services become obsolete. Use the **ipx sap follow-route-path** command to prevent the occurrence of SAP loops.

When the **ipx sap follow-route-path** command is used, the router screens individual services (SAPs) in SAP updates. The router looks at the destination network number of each SAP entry's . If the receiving interface is one of the best interfaces to reach the destination network of the SAP, that SAP entry is accepted. Otherwise, the SAP entry is discarded.



Caution

When the **ipx sap follow-route-path** command is globally enabled in conjunction with SAP input filters on interfaces that are considered the best paths to reach the destination networks, the SAPs that are being filtered will no longer be learned by the router, even if other less optimal interfaces are capable of receiving those SAP updates.

Examples

The following example enables the router to accept only the IPX SAP entries from SAP updates received on an interface deemed to be one of the best paths to the destination address of those SAPs:

```
ipx sap follow-route-path
```

Related Commands

Command	Description
ipx server-split-horizon-on-server-paths	Controls whether Service Information split horizon checking should be based on RIP or SAP.

ipx sap-helper

To set an address, which should be another Cisco router that is adjacent to the router being configured, to which all Service Advertising Protocol (SAP) request packets are received, use the **ipx sap-helper** command in interface configuration mode. To remove the address and stop forwarding SAP request packets, use the **no** form of this command.

ipx sap-helper *network.node*

no ipx sap-helper *network.node*

Syntax Description

network.node

The argument *network* is the network on which the SAP helper router resides. This eight-digit hexadecimal number uniquely identifies a network cable segment. It can be a number in the range from 1 to FFFFFFFD. You do not need to specify the leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

The argument *node* is the node number of the SAP helper router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxx.xxxx.xxx*).

Defaults

No helper address is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

Use this command to redirect SAP packet requests that are sent to a remote router that has a limited memory size, CPU speed, and often a slow WAN link joining it to the main corporate backbone. The SAP helper target is usually much a much larger router that has a much larger routing table and a complete SAP table.

Examples

The following example assigns a router with the address 1000.0000.0c00.1234 as the SAP helper:

```
interface ethernet 0
 ipx sap-helper 1000.0000.0c00.1234
```

Related Commands

Command	Description
ipx helper-address	Forwards broadcast packets to a specified server.