

# ipx sap-incremental (EIGRP)

To send Service Advertising Protocol (SAP) updates only when a change occurs in the SAP table, use the **ipx sap-incremental** command in interface configuration mode. To send periodic SAP updates, use the **no** form of this command.

**ipx sap-incremental eigrp** *autonomous-system-number* [**rsup-only**]

**no ipx sap-incremental eigrp** [**rsup-only**]

## Syntax Description

<i>autonomous-system-number</i>	IPX Enhanced IGRP autonomous system number. It can be a number from 1 to 65535.
	(Optional) Indicates that the system uses Enhanced IGRP on this interface to carry reliable SAP update information only. RIP routing updates are used, and Enhanced IGRP routing updates are ignored.

## Defaults

Enabled on serial interfaces

Disabled on LAN media (Ethernet, Token Ring, FDDI)

## Command Modes

## Command History

Release	Modification
10.0	This command was introduced.

## Usage Guidelines

When using the **ipx sap-incremental eigrp** command, you must enable Enhanced IGRP. This is the case even if you want to use only RIP routing. You must do this because the incremental SAP feature requires the Enhanced IGRP reliable transport mechanisms.

With this functionality enabled, if an IPX Enhanced IGRP peer is found on the interface, SAP updates will be sent only when a change occurs in the SAP table. Periodic SAP updates are not sent. When no IPX Enhanced IGRP peer is present on the interface, periodic SAPs are always sent, regardless of how this command is set.

If you configure the local router to send incremental SAP updates on an Ethernet, and if the local device has at least one IPX Enhanced IGRP neighbor and any servers, clients, or routers that do not have IPX Enhanced IGRP configured on the Ethernet interface, these devices will not receive complete SAP information from the local router.

If the incremental sending of SAP updates on an interface is configured and no IPX Enhanced IGRP peer is found, SAP updates will be sent periodically until a peer is found. Then, updates will be sent only when changes occur in the SAP table.

---

To take advantage of Enhanced IGRP's incremental SAP update mechanism while using the RIP routing protocol instead of the Enhanced IGRP routing protocol, specify the `rip` keyword. SAP updates are then sent only when changes occur, and only changes are sent. Use this feature only when you want to use RIP routing; Cisco IOS software disables the exchange of route information via Enhanced IGRP for that interface.

---

**Examples**

The following example sends SAP updates on Ethernet interface 0 only when there is a change in the SAP table:

```
interface ethernet 0
 ipx sap-incremental eigrp 200
```

# ipx sap-incremental split-horizon

To configure incremental SAP split horizon, use the `split-horizon` command, or to disable it, use the `no` command.

**ipx sap-incremental split-horizon**

**no ipx sap-incremental split-horizon**

Release	Modification
12.0	This command was introduced.



## Caution

%IPX EIGRP not running.

routers, particularly when links are broken. However, with nonbroadcast networks, such as Frame Relay and SMDS, situations can arise for which this behavior is less than ideal. For these situations, you may wish to disable split horizon.



## Note

## Examples

```
no ipx sap-incremental split-horizon
```

---

---

---

---

---

---

**show ipx eigrp neighbors**

---

---

# ipx sap-max-packetsize

```
ipx sap-max-packetsize  
no
```

```
ipx sap-max-packetsize
```

```
no ipx sap-max-packetsize
```

---

---

---

480 bytes

---

Interface configuration

---

---

---

---

The maximum size is for the IPX packet, including the IPX network and SAP header information. For example, to allow 10 servers per SAP packet, you would configure  $(32 + (10 \times 64))$ , or 672 bytes for the maximum packet size.

You are responsible for guaranteeing that the maximum packet size does not exceed the allowed maximum size of packets for the interface.

---

The following example sets the maximum SAP update packet size to 672 bytes:

```
ipx sap-max-packetsize 672
```

---

---

---

# ipx sap-multiplier

*multiplier*

*multiplier*

---

*multiplier*

---

aging-out interval. The default is three times the SAP update interval.

---

---

10.3

This command was introduced.

---

---

```
ipx sap-multiplier 10
```

---

---

Configures the maximum packet size of SAP updates sent out the interface.

---

# ipx sap-queue-maximum

```
ipx sap-queue-maximum
no
```

```
ipx sap-queue-maximum queue maximum
```

```
queue maximum
```

---

---

---

---

---

---

---

---

SAP request packets are dropped. Be sure to set a large enough queue limit to handle normal incoming SAP requests on all interfaces, or else the SAP information may time out.

---

The following example sets a SAP queue maximum of 500 milliseconds:

```
ipx sap-queue-maximum 500
```

---

---

---

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

---

**ipx sap-update-queue-maximum**

---

# ipx sap-update-queue-maximum

---

## Syntax Description

---

---

## Defaults

---

---

## Command Modes

---

---

## Command History

---

---

---

## Usage Guidelines



### Note

---

## Examples

```
ipx sap-update-queue-maximum 500
```

| \_\_\_\_\_ ■

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

# ipx server-split-horizon-on-server-paths

```
ipx server-split-horizon-on-server-paths
no
ipx server-split-horizon-on-server-paths
no ipx server-split-horizon-on-server-paths
```

---

---

---

---

---

---

---

---

---

---

**ipx server-split-horizon-on-server-paths**

---

---

```
ipx server-split-horizon-on-server-paths
```

---

---

---

---

---

---

---

# ipx split-horizon eigrp

---

## Syntax Description

---

---

## Defaults

---

## Command Modes

---

## Command History

---

Release	Modification
---------	--------------

---

---

## Usage Guidelines

---

## Examples

# ipx spx-idle-time

*delay-in-seconds*

---

---

---

---

---

---

---

---

---

---

**ipx spx-spoof**

---

```
ipx spx-idle-time 300
```

| \_\_\_\_\_ ■

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

| \_\_\_\_\_ ■

# ipx spx-spoof

| *table-clear-hours*

---

Sets the time to clear inactive entries. Values are 0 through 4,294,967,295.

---

Sets the time to clear the SPX table.

---

(Optional) Number of minutes before inactive entries are cleared from the session. Values are 0 through 4,294,967,295.

---

(Optional) Number of hours before the IPX table is cleared. Values are 0 through 4,294,967,295.

---

---

11.0

This command was introduced.

---

server's keepalive packets on a remote client's behalf. This is sometimes referred to as "spoofing the server."

You can use the `table-clear-hours` command to set the elapsed time in seconds after which spoofing of keepalive packets occurs, following the end of data transfer. If you turn on SPX spoofing and you do not set an idle time, the default of 60 seconds is assumed. This means that the dialer idle time begins

when SPX spoofing begins. For example, if the dialer idle time is 3 minutes, the elapse time before the line goes “idle-spoofing” is 4 minutes: 3 minutes of dialer idle time plus 1 minute of SPX spoofing idle time.

---

The following example enables spoofing on serial interface 0:

---

---

Configures the throughput.

---

Displays the table of SPX connections through interfaces for which SPX spoofing is enabled.

---

To configure the throughput, use the \_\_\_\_\_ command in interface configuration mode. To revert to the current bandwidth setting for the interface, use the \_\_\_\_\_ form of this command.

---

Throughput, in bits per second.

---

---

Current bandwidth setting for the interface

---

Interface configuration

---

10.3 \_\_\_\_\_ This command was introduced.

---

---

The value you specify with the \_\_\_\_\_ command overrides the value measured by IPXWAN when it starts. This value is also supplied to NLSP for use in its metric calculations.

---

The following example changes the throughput to 1,000,000 bits per second:

---

Enables the IPXWAN protocol on a serial interface.

---

# ipx triggered-rip-delay

[ ]

---

Delay, in milliseconds, between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

---



---

55 ms

---

Interface configuration

---



---

11.1 This command was introduced.

---



---

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. A triggered routing update is one that the system sends in response to a “trigger” event, such as a request packet, interface up/down, route up/down, or server up/down.

The `ipx triggered-rip-delay` command sets the interpacket delay for triggered routing updates sent on a single interface. The delay value set by this command overrides the delay value set by the `ipx rip-delay` or `ipx rip-interval` command for triggered routing updates sent on the interface.

If the delay value set by the `ipx rip-delay` or `ipx rip-interval` command is high, then we strongly recommend a low delay value for triggered routing updates so that updates triggered by special events are sent in a more timely manner than periodic routing updates.

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.

When you do not set the interpacket delay for triggered routing updates, the system uses the delay specified by the `ipx rip-delay` or `ipx rip-interval` command for both periodic and triggered routing updates.

When you use the `ipx triggered-rip-delay` form of the `ipx triggered-rip-delay` command, the system uses the global default delay set by the `ipx triggered-rip-delay` command for triggered RIP updates, if it is set. If it is not set, the system uses the delay set by the `ipx triggered-rip-delay` or `ipx triggered-rip-delay` command for triggered RIP updates, if set. Otherwise, the system uses the initial default delay as described in the “Defaults” section.

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

---

The following example sets an interpacket delay of 55 ms for triggered routing updates sent on interface FDDI 0:

```
interface FDDI 0
 ipx triggered-rip-delay 55
```

---

---

---

---

---

---

# ipx triggered-rip-holddown

---

## Syntax Description

---

---

## Defaults

---

---

## Command Modes

---

---

## Command History

---

---

---

## Usage Guidelines

---

---

## Examples

```
ipx triggered-rip-holddown 100
```

---

---

---

---

---



---

---

---

---

---

---

---

---

---

---







---

---

---

---

---

---

---

---

---

---

---

```
interface ether 0  
ipx triggered-sap-holddown 100
```

---

---

---

---

---

---



# ipx type-20-helpered

type-20-helpered

no

ipx type-20-helpered

no ipx type-20-helpered

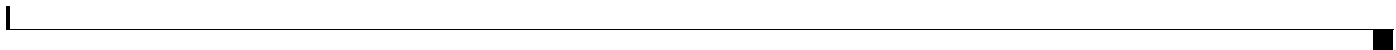
ipx type-20-helpered  
ipx type-20-propagation  
ipx type-20-propagation

ipx type-20-helpered  
ipx helper-address

ipx type-20-helpered

ipx helper-address bb.ffff.ffff.ffff





---

---

---

---

---

---

---

---

---

ipx type-20-input-checks

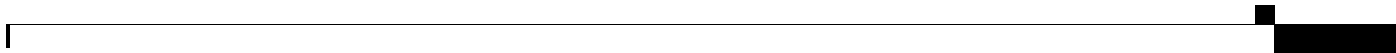
---

---

---

---

---





---

---

---

---

---

---

---

---

---

ipx type-20-output-checks

---

---

---

---

---



---

---

---

---

---

---

---

command. Note that type 20 packets are subject to loop detection and control as specified in the IPX router specification.

Additional input and output checks may be imposed by the `ipx type-20-propagation` and `ipx type-20-accept` commands.

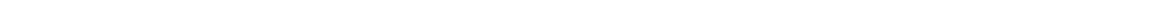
IPX type 20 propagation packet broadcasts are subject to any filtering defined by the `ipx type-20-filter` command.

---

The following example enables both the reception and forwarding of type 20 broadcasts on Ethernet interface 0:

The following example enables the reception and forwarding of type 20 broadcasts between networks 123 and 456, but does not enable reception and forwarding of these broadcasts to and from network 789:

```
!
interface ethernet 1
 ipx network 456
 ipx type-20-propagation
!
interface ethernet 2
 ipx network 789
```



{ | } {value}

<b>Release</b>	<b>Modification</b>

- 

-

**ipx update interval**

- 
- 
- 

---

**Examples**

---

**Related Commands**

---

**Command**

---

**Description**

---

---

---

---

---

---

# ipx update sap-after-rip

---

## Syntax Description

---

## Defaults

---

## Command Modes

---

## Command History

---

Release	Modification

---

---

## Usage Guidelines

---

## Examples

---

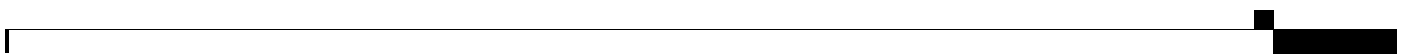
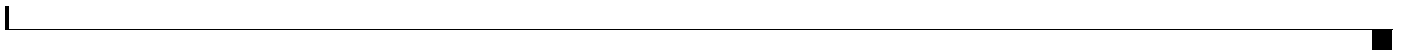
## Related Commands

---

Command	Description

---





# log-adjacency-changes (IPX)

```
log-adjacency-changes
no
```

```
log-adjacency-changes
```

```
no log-adjacency-changes
```

---

## Syntax Description

---



---



---



---



---



---



---

```
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

```
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0C34.D838 (Ethernet1.2) Down, hold time expired
%CLNS-5-MULTICAST: NLSP: Multicast address in use on Ethernet1.2
```

```
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0C34.D838 (Ethernet1.2) Up, new adjacency
%CLNS-5-MULTICAST: NLSP Broadcast address is in use on Ethernet1.2
```

---

*area1*

```
ipx router nlspl area1
log-adjacency-changes
```

| \_\_\_\_\_ ■

\_\_\_\_\_ ■  
\_\_\_\_\_  
\_\_\_\_\_

| \_\_\_\_\_ ■

# log-neighbor-changes (EIGRP)

---

## Syntax Description

---

## Defaults

---

## Command Modes

---

## Command History

---

---

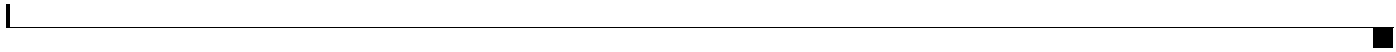
---

---

## Usage Guidelines

*as-number*                      *address interface*                      *state*   *reason*

<i>as-number</i>	
<i>address (interface)</i>	
<i>state</i>	
<i>reason</i>	



*seconds*

*seconds*

---

*seconds*

---

---

---

---

---

---

---

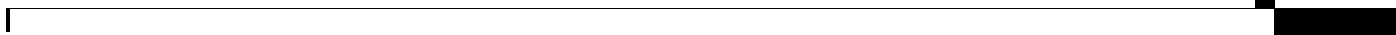
---

---

---

---

---





*bytes*

*bytes*



*bytes*



*seconds*

*seconds*

**max-lsp-lifetime (IPX)**

**ipx router**  
**max-lsp-lifetime**  
**(IPX)**

---

---

(Optional) If specified, the lifetime of the LSP is set in hours. If not specified, the lifetime is set in seconds.

---

Lifetime of LSP in hours or seconds. It can be a number in the range 1 to 32767. The default is 7500 seconds.

---

---

10.3 This command was introduced.

---

---

router to keep LSPs for a much longer time. Keeping LSPs longer reduces overhead on slower-speed serial links and keeps ISDN links from becoming active unnecessarily.

You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the router configuration command. The maximum LSP lifetime must be greater than the LSP refresh interval.

---

The following example sets the maximum time that the LSP persists to 11,000 seconds (more than 3 hours):

The following example sets the maximum time that the LSP persists to 15 hours:

---

---

Specifies the routing protocol to use.

---

Sets the LSP refresh interval.

---

---

To configure the router to use multicast addressing, use the `no ip multicast` command in router configuration mode. To configure the router to use broadcast addressing, use the `ip broadcast` form of this command.

---

This command has no arguments or keywords.

---

Multicast addressing is enabled.

---

Router configuration

---

11.3	This command was introduced.
------	------------------------------

---

---

This command allows the router 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 on any interface where multicast addressing is not supported by the hardware or driver.

---

The following example disables multicast addressing on the router:

To define an IPX NetBIOS FindName access list filter, use the `ipx netbios find-name` command in global configuration mode. To remove a filter, use the `no ipx netbios find-name` form of the command.

```
ipx netbios find-name { name | offset } string  
ipx netbios find-name name offset byte-pattern  
no ipx netbios find-name name offset byte-pattern
```

---

*name*

---

---

*string*

---

\*—Match one or more characters. You can use this wildcard character only at the end of a string.

?—Match any single character.

---

Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more `ipx netbios find-name` commands.

---

Decimal number that indicates the number of bytes into the packet at which the byte comparison should begin. An offset of 0 indicates the beginning of the NetBIOS packet header, which is at the end of the IPX header.

---

Hexadecimal pattern that represents the byte pattern to match. It can be up to 16 bytes (32 digits) long and must be an even number of digits. The argument `offset` can include the double asterisk (\*\*) wildcard character to match any digits for that byte.

---

---

10.0

This command was introduced.

---

---

Keep the following points in mind when configuring IPX NetBIOS access control:

Host (node) names are case-sensitive.

Host and byte access lists can have the same names. They are independent of each other.

When filtering by node name for IPX NetBIOS, the names in the access lists are compared with the destination name field for IPX NetBIOS “find name” requests.

When filtering by byte offset, note that these access filters can have a significant impact on the packets’ transmission rate across the bridge because each packet must be examined. You should use these access lists only when absolutely necessary.

If a node name is not found in an access list, the default action is to deny access.

These filters apply only to IPX NetBIOS FindName packets. They have no effect on LLC2 NetBIOS packets.

To delete an IPX NetBIOS access list, specify the minimum number of keywords and arguments needed to delete the proper list. For example, to delete the entire list, use the following command:

```
{ | }
```

To delete a single entry from the list, use the following command:

```
{ | }
```

---

The following example defines the IPX NetBIOS access list \_\_\_\_\_ :

The following example removes a single entry from the \_\_\_\_\_ access list:

The following example removes the entire \_\_\_\_\_ NetBIOS access list:

---

---

Controls incoming IPX NetBIOS FindName messages.

---

Controls outgoing NetBIOS FindName messages.

---

Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

---

To enable Enhanced IGRP, use the `ip igmp` (IPX Enhanced IGRP) command in router configuration mode. To disable Enhanced IGRP, use the `no ip igmp` form of this command.

`{network-number  
network-number`

---

`network-number`

---

---

*protocol source-network .source-node source-node-mask .source-node  
source-network-mask.source-node-mask source-socket  
destination-network .destination-node destination-node-mask .destination-node  
destination-network-mask.destination-node-mask destination-socket  
time-range-name*

*protocol source-network .source-node source-node-mask .source-node  
source-network-mask.source-node-mask source-socket  
destination-network .destination-node destination-node-mask .destination-node  
destination-network-mask.destination-nodemask destination-socket  
time-range-name*

---

*protocol*

---

*source-network*

---

*.source-node*

---

*source-node-mask*

*xxxx xxxx xxxx*

---

*source-node*

*xxxx xxxx xxxx*

---

*source-network-mask.*

*source-network*

*source-node-mask*

---

*source-socket*

---

---

*destination-network*

---

*.destination-node*

*xxxx xxxx xxxx*

---

*destination-node-mask*

*destination-node*

*xxxx xxxx xxxx*

---

*destination-network-mask.*

*destination-network*

*destination-node-mask*

---

*destination-socket*

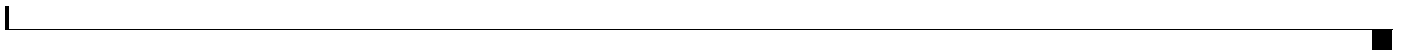
---

*time-range-name*

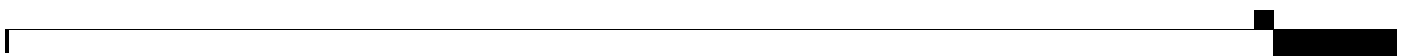
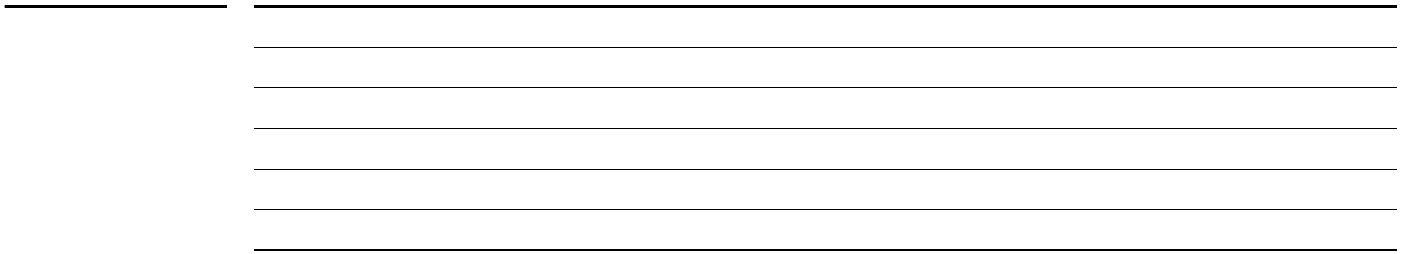
---

*time-range-name*

---



*sal*



*source-network .source-node source-node-mask  
destination-network .destination-node destination-node-mask*

*source-network .source-node source-node-mask  
destination-network .destination-node destination-node-mask*

---

*source-network*

---

*.source-node*

*xxxx xxxx xxxx*

---

*source-node-mask*

*source-node*

*xxxx xxxx xxxx*

---

*destination-network*

---

*.destination-node*

*xxxx xxxx xxxx*

---

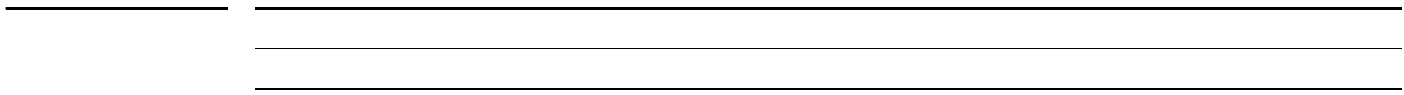
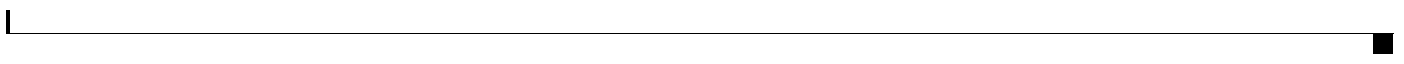
*destination-node-mask*

*destination-node*

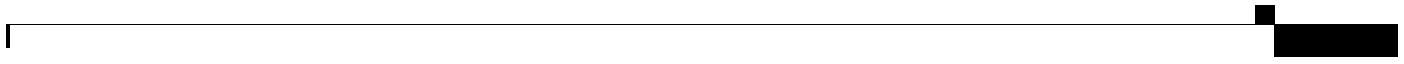
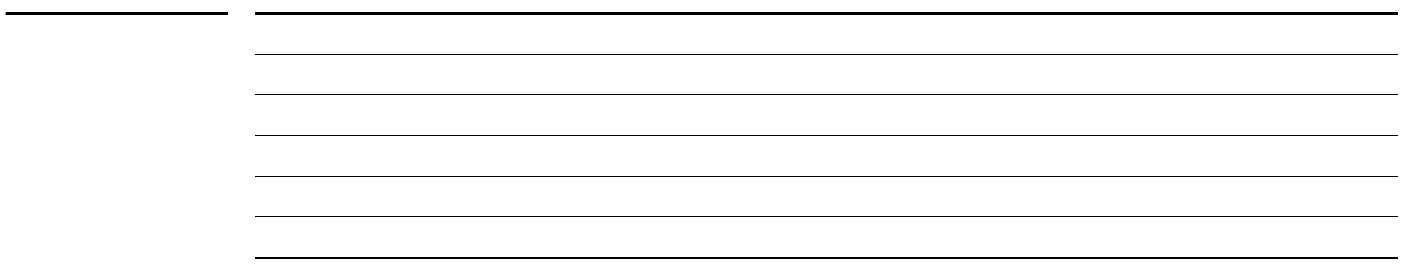
*xxxx xxxx xxxx*

---

---



*fred*



# permit (NLSP)

---

## Syntax Description

---

---

---

---

---

---

---

---

---

## Defaults

---

## Command Modes

---

## Command History

Release	Modification

---

## Usage Guidelines

---

**Examples**

---

**Related Commands**

---

<b>Command</b>	<b>Description</b>
----------------	--------------------

---

<b>access-list (NLSP)</b>	
---------------------------	--

---

<b>deny (NLSP)</b>	
--------------------	--

---

<b>ipx access-group</b>	
-------------------------	--

---

<b>ipx access-list</b>	
------------------------	--

---

<b>show ipx access-list</b>	
-----------------------------	--

---

# permit (SAP filtering)

**permit**  
**no**

**permit**  
**no permit**

---

## Syntax Description

network. A network number of -1 matches all networks.

You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

---

(Optional) Node on the network. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers ( . . ).

---

(Optional) Mask to be applied to the and arguments. Place ones in the bit positions to be masked.

---

(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.

---

(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (\*) at the end of the name as a wildcard to match one or more trailing characters.

---

---

## Defaults

---

## Command Modes

---

## Command History

---

11.3	This command was introduced.
------	------------------------------

---

---

## Usage Guidelines

**ipx access-list**

**access-list**

---

The following example creates a SAP access list named MyServer that allows only MyServer to be sent in SAP advertisements:

---

```
access-list (SAP filtering)
```

```
deny (SAP filtering)
```

```
ipx access-group
```

```
ipx access-list
```

```
show ipx access-list
```

---



**no prc-interval**

**prc-interval**

**no prc-interval**

---

---

---

---

---

---

---

---

**prc-interval**

**spf-interval**

---

---

**ipx router**

**spf-interval**

---



**redistribute**

**no**

**redistribute connected eigrp  
static**

**floating-static nosp rip**

**no redistribute connected eigrp  
static**

**floating-static nosp rip**

**redistribute eigrp  
access-list**

**nosp rip static**

**no redistribute eigrp  
access-list**

**nosp rip static**

---

**connected**

**eigrp**

---

**floating-static**

---

**nosp**

---

**rip**

---

**static**

**access-list**

---

**access-list**

---

---

---

---

---

---

---

**network**

**floating**

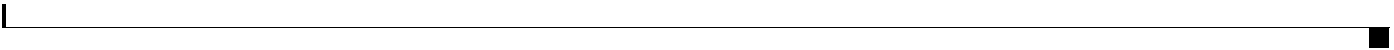
**ipx route**

**redistribute**



---

---



*area3*

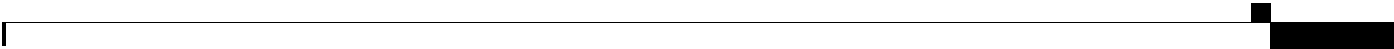
*aaaa0000\_ffff0000*

*a1*

*a2*

*a1*  
*a2*

*bbbb0000\_ffff0000*





---

---

---

---

---

---

---

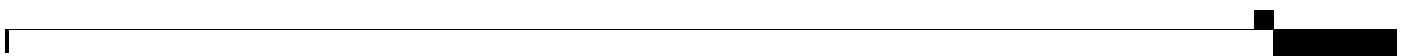
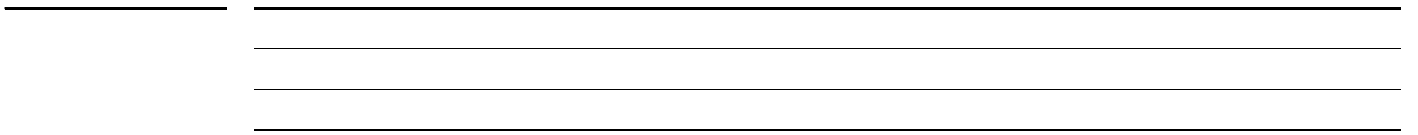
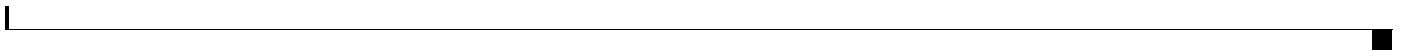
---



---

---





*access-list-number name*

```
Router# show ipx access-list
```

```
show ipx access-list London
```



**■ show ipx accounting****Related Commands****Command****Description**

Command	Description