6 IPX Router Commands

The following chapter contains information on Text-Based IPX Routing commands. Topics include:

- Configuring IPX Routing parameters
- Viewing IPX Routing information

Refer to the command task list below to find the page number for a specific task. If you would like to reference configuration tasks based on traditional UI commands, refer to Appendix A.

Command Tasks	
View data on IPX routing statistics and errors	6-3
View IPX Routing Table information	6-5
Add IPX static routes IPX Routing Table	6-7
Remove IPX static routes IPX Routing Table	6-8
Enable IPX routing	6-9
Disable IPX routing	6-10
Flush IPX RIP and SAP Bindery Tables	6-11
View listing of servers in SAP Bindery, sorted by server name	6-12
Test reachability of certain types of IPX nodes	6-14
Add IPX RIP output or input filter	6-16
Add IPX SAP output or input filter	6-17
Add IPX GNS output filter	6-19
Remove IPX RIP output or input filter	6-20
Remove IPX SAP output or input filter	6-21
Remove IPX GNS output filter	6-22
Display list of existing IPX RIP and SAP filters	6-23
Enable IPX Serialization Packet filtering on WAN routing services	6-24
Disable IPX Serialization Packet filtering on WAN routing services	6-25
View current status of IPX Serialization Packet filtering on WAN routing services	6-26
Enable IPX Watchdog Spoofing on any or all WAN routing services	6-27
Disable IPX Watchdog Spoofing on WAN routing services	6-28
View current status of IPX Watchdog Spoofing on WAN routing services	6-29
Enable SPX Keepalive Spoofing on WAN routing services	6-30
Disable SPX Keepalive Spoofing on WAN routing services	6-31

view ipx interface

Command Usage

View data on IPX routing statistics and errors.

Syntax Options

view ipx interface (No additional syntax options are used.)

Corresponding UI Command

ipxs

Screen Output

A screen similar to the following will be displayed:

```
IPX Statistics and Errors:

IPX is ON

IPX Input Statistics:
  pkts rcvd                 =  3280
  pkts delivered locally    =  3161
  pkts discarded            =  0
  input header errors       =  0

IPX Output Statistics:
  pkts sent                 =  4731
  pkts generated locally    =  4681
  pkts discarded            =  0
  pkts with no route found  =  1
  HRE pkts sent             =  0

There are 2 IPX interfaces defined.

Stats for IPX Router Interface on (Group:VLAN) 3:1, Net address 3333
  Interface name is IPX Router 3333
     state              =  ON          status       =  UP
     state changes      =  1500        type         =  BROADCAST
     rtr encapsulation  =  FD

     RIP is ON: sent = 1527, rcvd = 1568, update interval = 60 secs.
     SAP is ON: sent = 1, rcvd = 1568, update interval = 60 secs.

Stats for IPX Router Interface on (Group:VLAN) 4:1, Net address 5555
  Interface name is  IPX Router 5555
     state              =  ON          status       =  UP
     state changes      =  1500        type         =  BROADCAST
     rtr encapsulation  =  EN

     RIP is ON: sent = 1571, rcvd = 1, update interval = 60 secs.
     SAP is ON: sent = 1533, rcvd = 1, update interval = 60 secs.
```

Table Description

IPX. Indicates whether IPX routing is "ON" or "OFF."

pkts rcvd. The number of packets received.

pkts delivered locally. The number of received packets delivered to local IPX applications (RIP and SAP).

pkts discarded. The number of discarded packets.

input header errors. The number of packets discarded due to IPX packet header errors.

pkts sent. The number of packets forwarded (not including fast path routed packets).

pkts generated locally. The number of packets forwarded that were generated by local IPX applications (RIP and SAP).

pkts discarded. The number of discarded packets.

pkts with no route found. The number of packets that could not be forwarded because a route to the destination IPX network could not be found.

state. State of the IPX router for this interface (**on** or **off**).

status. Status of the interface (UP or DOWN).

type. The type of interface (BROADCAST or POINT-TO-POINT).

rtr encapsulation. Router port encapsulation used for this interface (EN=Ethernet, FD=FDDI, TR=Token Ring).

state changes. The number of state changes that have occurred on this interface (up to down, down to up).

sent. The number of RIP packets sent.

received. The number of RIP packets received.

update interval. The RIP update timer interval for this interface. If a WAN interface is configured as a Triggered RIP/SAP interface, this field will contain the word "triggered." Triggered interfaces transmit information only once, when the change occurs.

sent. The number of SAP packets sent.

received. The number of SAP packets received.

update interval. The SAP update timer interval for this interface. If a WAN interface is configured as a Triggered RIP/SAP interface, this field will contain the word "triggered." Triggered interfaces transmit information only once, when the change occurs.

view ipx route

Command Usage

View IPX Routing Table information.

Syntax Options

view ipx route [*ipx-network-number***] [***group:vlan [slot/port/dlci* | *ppp-peer-id]***]**

Definitions:
ipx-network-number = the destination IPX network number for a particular IPX route
group:vlan = specifies a group and VLAN ID for a particular IPX route
group:vlan slot/port/dlci = specifies a group and VLAN ID, in addition to slot, port, and virtual connection (DLCI).
group:vlan ppp-peer-id = specifies group and VLAN IDs, in addition to a PPP Peer ID

♦ Syntax Notes ♦

If you enter syntax options in the command line (IPX network number, group and VLAN ID, etc), information for only the corresponding route(s) will be displayed.

If you do *not* enter syntax options in the command line, the entire IPX Routing Table will be displayed.

Command Examples:
view ipx route 77:3
view ipx route 7:2 5/3/100
view ipx route 26dc012a
view ipx route P1
view ipx route

Corresponding UI Command

ipxr

Remarks

The entries in the IPX Routing Table show the routes entered by the IPX RIP protocol and the static routes that you may have entered manually. All entries in the table are sorted by destination network. The IPX Routing Table can contain a maximum of 2010 routes.

You can limit the number of routes that is displayed in the IPX Routing Table by including additional syntax options in the command line. (For more information, refer to the Syntax Options section below.)

Screen Output

A screen similar to the following will be displayed:

Displaying all (12) routes:

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc Peer ID
100	100.Direct	0	1	N	N	N	N	Y	3:1	
120	120.Direct	0	1	N	N	N	N	Y	4:1	
5000	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
5556	8484.0020da2200f4	1	2	N	N	N	N	N	6:1	P1
8484	8484.Direct	0	1	N	N	N	N	Y	6:1	
26dc012a	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/220
55555555	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
66666666	66666666.Direct	0	1	N	N	N	N	Y	5:1	
95000095	120.0020da092ef5	2	3	N	N	N	N	N	4:1	5/3/100

Table Description

Dest Net. The destination network IPX address.

Router. The IPX address (network.node) of the next hop router to reach the destination network.

Hops. The number of routers between this node and the destination network.

Delay. The number of "ticks" between this node and the destination network. A "tick" is about 1/18th of a second.

Static. Whether this route was statically defined.

Aged. Indicates if this route has timed out. Once a route times out it is kept in the routing table for 10 "ticks." Once the 10 "ticks" expire, the route is deleted.

Redir. Indicates that a route to an IPX network that was formerly reachable via a direct interface has been replaced by an alternate route.

Chg. The information in this route has recently been updated, but the new information has not yet been forwarded to neighbor routers.

Dir. Indicates that this is a local interface (direct route) as opposed to a route to a destination network.

GP:VL. The first number is the Group associated with this entry; the second number is the VLAN associated with this entry. This identifies the interface used when sending traffic to the destination network.

s/p/vc and **Peer ID.** (These fields are displayed only if a Frame Relay or ISDN module is installed on the switch.) The Slot, Port and Virtual Connection (i.e., DLCI) identifiers or the PPP Peer ID of the interface on which the routing information was received.

ipx route

Command Usage

Add IPX static routes to the switch's IPX Routing Table.

Syntax Options

ipx route <*network-number***> <***next-hop***> <***node-address***>**

Definitions:
network-number = the destination IPX address of the route you want to add (e.g., **26b**)
next-hop = the IPX network address of the next hop (e.g., **e8024**)
node-address = the IPX address of the network to which you are setting up the route (e.g., **00:20:da:d4:32:80**)

Command Example:
ipx route 26b e8024 00:20:de:d4:32:80

Corresponding UI Command

aipxsr

Remarks

In order to add a static route, you will need to know the host/net and the gateway which will be used to route traffic there.

no ipx route

Command Usage

Remove IPX static routes from the switch's IPX Routing Table.

Syntax Options

no ipx route <*network-number***>**

Definitions:
network-number = the destination IPX address for the route you want to remove (e.g., **e8024**)

Command Example:
no ipx route e8024

Corresponding UI Command

ripxsr

ipx routing

Command Usage

Turn on the IPX router complex, which enables IPX routing on the switch.

Syntax Options

ipx routing (No additional syntax options are used.)

Corresponding UI Command

ipxon

no ipx routing

Command Usage

Turn off the IPX router complex, which disables all IPX routing on the switch.

Syntax Options

no ipx routing (No additional syntax options are used.)

Corresponding UI Command

ipxoff

clear ipx route

Command Usage

Flush the IPX RIP and SAP Bindery Tables. You can choose to flush entries from *both* tables, or you can specify that only a particular table is flushed (i.e. RIP or SAP).

Syntax Options

clear ipx route [rip | sap | all]

Definitions:
all = flushes all entries from both the RIP and SAP Bindery tables
rip = flushes all entries from the RIP table only
sap = flushes all entries from the SAP table only

Command Default:
rip | sap | all = **all**

Command Examples:
clear ipx route
clear ipx route all
clear ipx route rip
clear ipx route sap

Corresponding UI Command

ipxflush

view ipx servers

Command Usage

View a listing of the servers in the SAP Bindery, sorted by server name.

Syntax Options

view ipx servers [*group:vlan***] [***server-name***] [***server-type***]**

Definitions:
group:vlan = a group and VLAN ID (e.g., **8:2**)
server-name = a server name (e.g., **Marketing**)
server-type = a hex-formatted service type (e.g., **26b**)

♦ Syntax Notes ♦

If you enter syntax options in the command line (group and VLAN ID, server name, server type), information for only the corresponding server(s) will be displayed.

If you do *not* enter syntax options in the command line, information for all servers will be displayed.

Command Examples:
view ipx servers
view ipx servers 77:3
view ipx servers Marketing
view ipx servers 0004
view ipx servers 4:2 0278
view ipx servers Finance 26b

Corresponding UI Command

ipxsap

Screen Output

A screen similar to the following will be displayed:

Displaying all (3) entries in the SAP bindery:

Server Name	Type	Address	Hp	Sckt	GP:VL	s/p/vc Peer ID
HR	0004	200.000000000022	1	0451	3:1	5/3/100
Sales	026b	200.000000000022	1	0005	2:1	5/3/220
Support	0278	200.000000000022	1	4006	2:1	5/3/220

Table Description

Server Name. The name of the server offering this service.

Type. The service type being offered (as defined by Novell).

Address. The IPX address of this server (network.node).

Hp. The number of networks between this node and the server.

Sckt. The Novell socket number to which this service is attached.

GP:VL. The first number is the Group associated with this entry, and the second number is the VLAN associated with this entry.

s/p/vc and **Peer ID.** (These fields are displayed only if a Frame Relay or ISDN module is installed on the switch.) The Slot, Port and Virtual Connection (i.e., DLCI) identifiers or the PPP Peer ID of the interface on which the server information was received.

ping ipx

Command Usage

Test the reachability of certain types of IPX nodes.

Syntax Options

ping ipx <*network-number***> <***node-address***> [***count***] [***size***] [***timeout***] [***type***]**

Definitions:
network-number = the destination network for the node that you want to ping
node-address = the destination node that you want to ping
count = the number of packets to be sent out. An entry of 0 will create an infinite count (press **enter** to cancel).
size = the number of data bytes included in each packet sent out
timeout = the number of seconds allowed for a response
type = the type of IPX ping to be issued (i.e., Novell or Xylan)

Defaults:
count = one (1) packet
size = sixty-four (64) bytes
timeout = one (1) second
type = Novell

Command Examples:
ping ipx 304 00:20:da:05:f6:94 0 32 2 xylan
ping ipx 304 00:20:da:05:f6:94 0
ping ipx 300 00:33:f8:90:50:da

Corresponding UI Command

ipxping

Remarks

The software supports two different types of IPX pings:

- a Novell-defined type that can test the reachability of NetWare servers currently running the NetWare Loadable Module called IPXRTR.NLM. This type *cannot* be used to reach NetWare workstations running IPXODI. Novell uses a unique type of ping for this purpose (implemented by their IPXPNG.EXE program) which is not currently supported by the switch software. Other vendor's switches may respond to this type of ping.
- a proprietary type that can test the reachability of Alcatel switches on which IPX routing has been enabled.

An important factor to keep in mind is that any network device that does not recognize the specific type of IPX ping request sent from the switch will not respond at all. However, the lack of a response does not necessarily mean that a specific network device is inactive or missing. Therefore, you might want to try using both types before concluding that the network device is "unreachable."

Screen Output

A screen similar to the following will be displayed:

```
IPX Ping starting, hit <RETURN> to stop
PING 304.00:20:da:05:f6:94: 64 data bytes

  [0              ] .

----304.00:20:da:05:f6:94 PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
```

ipx filter rip

Command Usage

Add an IPX RIP Output or Input filter.

Syntax Options

ipx filter [*group[:vlan]***] rip [in | out] [allow | block] [***address [mask]***]**

Definitions:
group = the IPX RIP filter will be added only to the specified group (e.g., **77**)
:*vlan* = the IPX RIP filter will be added only to the specified VLAN (e.g., **2**)
in = specifies *input* filter type
out = specifies *output* filter type
allow = the filter will allow traffic
block = the filter will block traffic
address = the IPX network address to be used (e.g., **e8024**)
mask = the IPX network mask to be used (e.g., **abcdef01**)

♦ Syntax Note ♦
If you enter a VLAN ID in the command line, you must type a colon (**:**) between the group number and VLAN number (e.g., **4:1**).

Command and Switch Defaults:
in | out = out
allow | block = allow
address [mask] = all networks

Command Examples:
ipx filter 3:2 rip in block e8024 abcdef01
ipx filter rip e8024
ipx filter rip block
ipx filter rip

Corresponding UI Command

ipxfilter

Remarks

The IPX RIP Filtering feature gives you a means of controlling the operation of the IPX RIP protocol. By using IPX RIP filters, you can minimize the number of entries put in the IPX RIP Routing Table, improve overall network performance by eliminating unnecessary traffic, and control users' access to NetWare services.

Two types of IPX RIP filters are available:

1. **RIP Input** filters control which networks are allowed into the routing table when IPX RIPs are received.
2. **RIP Output** filters control the list of networks included in routing updates sent out an interface. These filters control which networks the router advertises in its IPX RIP updates.

ipx filter sap

Command Usage

Add an IPX SAP Output or Input filter.

Syntax Options

ipx filter [*group[:vlan]***] sap {all |** *sap-type***} [in | out] [allow | block] [***network [mask]***] [***node [node-mask]***]**

Definitions:
group = the IPX SAP filter will be added only to the specified group (e.g., **77**)
:*vlan* = the IPX SAP filter will be added only to the specified VLAN (e.g., **2**)
all = specifies all SAP service types
sap-type = the 4-hex SAP service type as defined by NetWare (e.g., **00:20:DA:D4:32:80**).
in = specifies *input* filter type
out = specifies *output* filter type
allow = the filter will allow traffic
block = the filter will block traffic
network = the IPX network address to be used (e.g., **e8024**)
mask = the IPX network mask to be used (e.g., **abcdef01**)
node = the IPX node address to be used (e.g., **e8024**)
node-mask = the IPX node mask to be used (e.g., **abcdef01**)

♦ Syntax Note ♦
If you enter a VLAN ID in the command line, you must type a colon (**:**) between the group number and VLAN number (e.g., **4:1**).

Defaults:
in | out = **out**
allow | block = **allow**
network [mask] = all networks
node [node-mask] = all nodes

Command Examples:
ipx filter 3:2 sap all in block e8024 abcdef01
ipx filter sap 00:20:DA:D4:32:80 e8024
ipx filter sap all block
ipx filter sap all

Corresponding UI Command

ipxfilter

Remarks

The IPX SAP Filtering feature give you a means of controlling the operation of the IPX SAP protocol. By using IPX SAP filters, you can minimize the number of entries put in the IPX SAP Bindery Table, improve overall network performance by eliminating unnecessary traffic, and control users' access to NetWare services. Two types of IPX SAP filters are available:

1. **SAP Input** filters control the SAPs received by the router prior to a router accepting information about a service. The router will filter all incoming service advertisements received before accepting information about a service.

2. **SAP Output** filters control which services are included in SAP updates sent by the router. The router applies the SAP output filters prior to sending SAP packets.

ipx filter gns

Command Usage

Add an IPX GNS Output filter.

Syntax Options

ipx filter [*group[:vlan]***] gns {all |** *gns-type***} [out] [allow | block] [***network [mask]***] [***node [node-mask]***]**

Definitions:
group = the IPX GNS filter will be added only to the specified group (e.g., **77**)
:*vlan* = the IPX GNS filter will be added only to the specified VLAN (e.g., **2**)
all = specifies all GNS service types
gns-type = the 4-hex GNS service type as defined by NetWare (e.g., **00:20:DA:D4:32:80**).
out = specifies *output* filter type (GNS supports output filters only)
allow = the filter will allow traffic
block = the filter will block traffic
network = the IPX network address to be used (e.g., **e8024**)
mask = the IPX network mask to be used (e.g., **abcdef01**)
node = the IPX node address to be used (e.g., **e8024**)
node-mask = the IPX node mask to be used (e.g., **abcdef01**)

♦ Syntax Note ♦
If you enter a VLAN ID in the command line, you must type a colon (**:**) between the group number and VLAN number (e.g., **4:1**).

Command Defaults:
allow | block = **allow**
network [mask] = all networks
node [node-mask] = all nodes

Command Examples:
ipx filter 3:2 gns all block e8024
ipx filter gns 00:20:DA:D4:32:80 e8024
ipx filter gns all block
ipx filter gns all

Corresponding UI Command

ipxfilter

Remarks

GNS Output filters control which servers are included in the GNS responses sent by the router.

no ipx filter rip

Command Usage

Remove an IPX RIP output or input filter.

Syntax Options

no ipx filter [*group[:vlan]***] rip [in | out] [allow | block] [***network [mask]***]**

Definitions:
group = the IPX RIP filter will be removed from the specified group (e.g., **77**)
:*vlan* = the IPX RIP filter will be removed from the specified VLAN (e.g., **:2**)
in = specifies *input* filter type
out = specifies *output* filter type
allow = the filter to be removed currently allows traffic
block = the filter to be removed currently blocks traffic
network = the current IPX network address (e.g., **e8024**)
mask = the current IPX network mask (e.g., **abcdef01**)

♦ Syntax Note ♦
If you enter a VLAN ID in the command line, you must type a colon (**:**) between the group number and VLAN number (e.g., **4:1**).

Command Defaults:
in | out = **out**
allow | block = **allow**
network = all networks

Command Examples:
no ipx filter 3:2 rip in block e8024 abcdef01
no ipx filter rip e8024
no ipx filter rip block
no ipx filter rip

Corresponding UI Command

ipxfilter

no ipx filter sap

Command Usage

Remove an IPX SAP output or input filter.

Syntax Options

no ipx filter [*group[:vlan]***] sap {all |** *sap-type***} [in | out] [allow | block] [***network [mask]***] [***node [node-mask]***]**

Definitions:
group = the IPX SAP filter will be removed from the specified group (e.g., **77**)
:*vlan* = the IPX SAP filter will be removed from the specified VLAN (e.g., **:2**)
all = specifies all SAP service types
sap-type = the 4-hex SAP service type as defined by NetWare (e.g., **00:20:DA:D4:32:80**).
in = specifies *input* filter type
out = specifies *output* filter type
allow = the filter to be removed currently allows traffic
block = the filter to be removed currently blocks traffic
network = the current IPX network address (e.g., **e8024**)
mask = the current IPX network mask (e.g., **abcdef01**)
node = the IPX node address to be used (e.g., **e8024**)
node-mask = the IPX node mask to be used (e.g., **abcdef01**)

♦ Syntax Note ♦
If you enter a VLAN ID in the command line, you must type a colon (**:**) between the group number and VLAN number (e.g., **4:1**).

Command Defaults:
in | out = **out**
allow | block = **allow**
network [mask] = all networks
node [node-mask] = all nodes

Command Examples:
no ipx filter 3:2 sap all in block e8024 abcdef01
no ipx filter sap 00:20:DA:D4:32:80 e8024
no ipx filter sap all block
no ipx filter sap all

Corresponding UI Command

ipxfilter

no ipx filter gns

Command Usage

Remove an IPX GNS Output filter.

Syntax Options

no ipx filter [*group[:vlan]***] gns {all | *gns-type*} [out] [allow | block] [***network [mask]***] [***node [node-mask]***]**

Definitions:
group = the IPX GNS filter will be removed from the specified group (e.g., **77**)
:*vlan* = the IPX GNS filter will be removed from the specified VLAN (e.g., **:2**)
all = specifies all GNS service types
sap-type = the 4-hex GNS service type as defined by NetWare (e.g., **00:20:DA:D4:32:80**).
in = specifies *input* filter type
out = specifies *output* filter type
allow = the filter to be removed currently allows traffic
block = the filter to be removed currently blocks traffic
network = the current IPX network address (e.g., **e8024**)
mask = the current IPX network mask (e.g., **abcdef01**)
node = the IPX node address to be used (e.g., **e8024**)
node-mask = the IPX node mask to be used (e.g., **abcdef01**)

♦ Syntax Note ♦
If you enter a VLAN ID in the command line, you must type a colon (**:**) between the group number and VLAN number (e.g., **4:1**).

Command Defaults:
allow | block = **allow**
network [mask] = all networks
node [node-mask] = all nodes

Command Examples:
no ipx filter 3:2 gns all block e8024
no ipx filter gns 00:20:DA:D4:32:80 e8024
no ipx filter gns all block
no ipx filter gns all

Corresponding UI Command

ipxfilter

view ipx filter

Command Usage

Display a list of existing IPX RIP and SAP filters. You can choose to view all IPX filters or specific IPX filters.

Syntax Options

view ipx filter [*group*:*vlan* **| rip in | rip out | sap in | sap out | gns out | global]**

Definitions:
group:*vlan* = displays filter information for a specific VLAN
rip in = displays information on RIPs received
rip out = displays information on RIPs sent
sap in = displays information on SAPs received
sap out = displays information on SAPs sent
gns out = displays information on GNS responses sent
global = displays RIP, SAP, and GNS filter information for all router interfaces

Defaults:
group:*vlan* **| rip in | rip out | sap in | sap out | gns out | global** = **global**

Command Examples:
view ipx filter
view ipx filter global
view ipx filter rip out
view ipx filter 5:3

Corresponding UI Command

ipxf

Screen Output

A screen similar to the following will be displayed:

```
Displaying all filters:

                                                                                GP:VL  (s/p/vc)
  #     Type          Net/Mask          Node/Mask                    Svc   Md          (Peer ID)
------  ------------  ----------------------  ---------------------------------  ------  ----  --------------------
   1    SAP OUT       67/ffffffff       000000000001/ffffffffffff     ALL     B   global
   2    SAP IN        67/ffffffff       000000000001/ffffffffffff     0278    B   1:1
   3    RIP IN        67/ffffffff                                             B   global
   4    SAP IN        All Networks                    All Nodes       ALL     B   3:1 (P1)
```

ipx serialization

Command Usage

Enable IPX serialization packet filtering on any or all WAN routing services.

Syntax Options

ipx serialization {*group-number* **| all}**

Definitions:
group-number = specifies the group for which you would like to enable IPX serialization (e.g., **4**)
all = specifies that IPX serialization will be enabled for *all* WAN routing services

Command Examples:
ipx serialization 77
ipx serialization all

Corresponding UI Command

ipxserialf

Remarks

This feature can be used to reduce traffic on WAN links by preventing the transmission of NetWare serialization packets.

Novell uses a serialization mechanism to make sure that licensed copies of NetWare are not improperly copied to multiple servers. NetWare's built-in copy protection scheme transmits serialization packets between file servers which contain unique serialization numbers. These packets are sent out at about 66-second intervals. If a server detects duplicate serialization identifiers, it broadcasts a copyright violation message to all users and to the console log. The major problem with this protection scheme for dial-on-demand links, such as ISDN, is the generation of traffic that continuously reactivates the WAN link.

no ipx serialization

Command Usage

Disable IPX serialization packet filtering on any or all WAN routing services.

Syntax Options

no ipx serialization {*group-number* **| all}**

Definitions:
group-number = specifies the group for which you would like to disable IPX serialization (e.g., **4**)
all = specifies that IPX serialization will be disabled for *all* WAN routing services

Command Examples:
no ipx serialization 4
no ipx serialization all

Corresponding UI Command

ipxserialf

view ipx serialization

Command Usage

View the current status of IPX serialization packet filtering on WAN routing services.

Syntax Options

view ipx serialization (No additional syntax options are used.)

Screen Output

A screen similar to the following will be displayed:

```
Group      IPX Serialization Filtering
---------- ---------------------------------------
3                     Disabled
4                     Disabled
```

Corresponding UI Command

ipxserialf

ipx watchdog-spoof

Command Usage

Enable IPX Watchdog Spoofing on any or all WAN routing services.

Syntax Options

ipx watchdog-spoof {*group-number* **| all}**

Definitions:
group-number = the group for which you would like to enable IPX Watchdog Spoofing (e.g., **3**)
all = specifies that IPX Watchdog Spoofing will be enabled for *all* WAN routing services

Command Examples:
ipx watchdog-spoof 3
ipx watchdog-spoof all

Corresponding UI Command

ipxspoof

Remarks

Novell's IPX Watchdog Protocol, which is used by NetWare to maintain network node and server connections, can consume significant network bandwidth and thereby incur costs on expensive dial-on-demand, pay-per-packet WAN links. The switch provides an IPX Watchdog Spoofing feature to prevent Watchdog packets from initiating connections on WAN links in situations where no other data is ready to be transferred.

The IPX Watchdog Spoofing feature enables the switch to respond to a NetWare server's Watchdog "Query" requests on behalf of a remote client, thus spoofing the requests. The spoofing action occurs when the switch "sees" an incoming Watchdog packet destined for an interface on which spoofing has been enabled. The switch responds to the server by sending out a valid Watchdog response. Spoofing thus maintains the required Watchdog function while avoiding the cost of making and maintaining a WAN link.

In some situations, the use of the IPX Watchdog Spoofing feature can make a NetWare server "believe" that an inactive session is still active. This occurrence can cause connectivity problems by denying login rights to legitimate users. Therefore, if you use the spoofing feature on networks that also limit the number of IPX or SPX sessions, you should utilize NetWare's "auto-logoff" function to minimize inappropriate denials of legitimate logins.

no ipx watchdog-spoof

Command Usage

Disable IPX Watchdog Spoofing on any or all WAN routing services.

Syntax Options

no ipx watchdog-spoof {*group-number* **| all}**

Definitions:
group-number = the group on which you would like to disable IPX Watchdog Spoofing (e.g., **4**)
all = specifies that IPX Watchdog Spoofing will be disabled on *all* WAN routing services

Command Examples:
no ipx watchdog-spoof 4
no ipx watchdog-spoof all

Corresponding UI Command

ipxspoof

view ipx watchdog-spoof

Command Usage

View the current status of IPX Watchdog Spoofing on WAN routing services.

Syntax Options

view ipx watchdog-spoof (No additional syntax options are used.)

Screen Output

A screen similar to the following will be displayed:

```
Group          IPX Spoofing
-----------    ----------------------------
3                    Disabled
4                    Disabled
```

Corresponding UI Command

ipxspoof

ipx spx-spoof

Command Usage

Enable SPX Keepalive Spoofing on any or all WAN routing services.

Syntax Options

ipx spx-spoof {*group-number* | **all}**

Definitions:
group-number = the group for which you would like to enable SPX Keepalive Spoofing (e.g., **3**)
all = specifies that SPX Keepalive Spoofing will be enabled for *all* WAN routing services

Command Examples:
ipx spx-spoof 3
ipx spx-spoof all

Corresponding UI Command

spxspoof

Remarks

Novell's SPX Keepalive Protocol, which is used by NetWare to maintain SPX connections between end nodes, can also consume significant network bandwidth and thereby incur unnecessary costs on expensive dial-on-demand, pay-per-packet WAN links. The switch provides an SPX Keepalive Spoofing feature to prevent keepalive packets from keeping WAN links active when they are not otherwise needed for data transmissions.

The SPX Spoofing feature enables the switch to respond to client/server keepalive packets on the behalf of the remote clients/servers. SPX spoofing thereby effectively stops keepalive packets from crossing a WAN link while maintaining existing SPX connections.

no ipx spx-spoof

Command Usage

Disable SPX Keepalive Spoofing on any or all WAN routing services.

Syntax Options

no ipx spx-spoof {*group-number* | **all}**

Definitions:
group-number = specifies the group for which you would like to disable SPX Keepalive Spoofing (e.g., **4**)
all = specifies that SPX Keepalive Spoofing will be disabled for *all* WAN routing services

Command Examples:
no ipx spx-spoof 4
no ipx spx-spoof all

Corresponding UI Command

spxspoof

view ipx spx-spoof

Command Usage

View the current status of SPX Keepalive Spoofing on WAN routing services.

Syntax Options

view ipx spx-spoof (No additional syntax options are used.)

Screen Output

A screen similar to the following will be displayed:

```
Group          SPX Spoofing
----------     ----------------------------
3                    Disabled
4                    Disabled
```

Corresponding UI Command

spxspoof

ipx type-20-propagation

Command Usage

Enable IPX Type 20 packet forwarding.

Syntax Options

ipx type-20-propagation <*group:vlan***>**

Definitions:
group:vlan = specifies the group and VLAN on which Type 20 packet forwarding is to be enabled (e.g, **3:2**)

Command Examples:
ipx type-20-propagation 3:2

Corresponding UI Command

ipxtype20

Remarks

Type 20 packets contain the value 20 (14 hex) in the "packet type" field of the IPX header. Novell has defined the use of these packets to support certain protocol implementations, such as NetBIOS. As these packets are broadcasted and propagated across networks, the addresses of those networks (up to 8) are stored in the packet's data area.

Type 20 packet forwarding is turned *off* by default because it can cause problems in highly redundant IPX networks by causing what appears to be a broadcast storm. This problem is aggravated whenever misconfigured PCs are added to a network.

no ipx type-20-propagation

Command Usage

Disable IPX Type 20 packet forwarding.

Syntax Options

no ipx type-20-propagation <*group:vlan***>**

Definitions:
group:vlan = the group and VLAN on which Type 20 packet forwarding is to be disabled (e.g, **3:2**)

Command Examples:
no ipx type-20-propagation 3:2

Corresponding UI Command

ipxtype20

view ipx type-20-propagation

Command Usage

View the current status of IPX Type 20 packet forwarding.

Syntax Options

view ipx type-20-propagation (No additional syntax options are used.)

Corresponding UI Command

ipxtype20

Screen Output

A screen similar to the following will be displayed:

```
GP:VL     Type20 Packet Forwarding
-------   ----------------------------------------
 3:1       off
 4:1       off
```

ipx default-route

Command Usage

Add an IPX default route.

Syntax Options

ipx default-route <*network-number***> <***node-address***>**

Definitions:
network-number = the destination network location for the default route (e.g., **222**)
node-address = the destination node for the default route (e.g., **00:20:da:99:88:77**)

Command Example:
ipx default-route 222 00:20:da:99:88:77

Corresponding UI Command

ipxdrt

Remarks

A default IPX route may be configured for packets destined for networks that are unknown to the switch. If RIP messages are disabled, packets can still be forwarded to a router that knows where to send them.

no ipx default-route

Command Usage

Delete a default route.

Syntax Options

no ipx default-route (No additional syntax options are used.)

Corresponding UI Command

ipxdrt

view ipx default-route

Command Usage

View the status of a default route.

Syntax Options

view ipx default-route (No additional syntax options are used.)

Corresponding UI Command

ipxdrt

Screen Output

A screen similar to the following will be displayed:

```
IPX default route:   00000222   00:20:da:99:88:77
```

ipx packet-extension

Command Usage

Enable extended RIP and SAP packets.

Syntax Options

ipx packet-extension (No additional syntax options are used.)

Corresponding UI Command

ipxext

Remarks

Larger RIP and SAP packets may be transmitted so that congestion in the network is reduced. Other switches and routers in the network must support a larger—or *extended*—packet size if this feature is configured on the switch.

no ipx packet-extension

Command Usage

Disable extended RIP and SAP packets.

Syntax Options

no ipx packet-extension (No additional syntax options are used.)

Corresponding UI Command

ipxext

view ipx packet-extension

Command Usage

View the current status of extended RIP and SAP packets.

Syntax Options

view ipx packet-extension (No additional syntax options are used.)

Corresponding UI Command

ipxext

Screen Output

If extended RIP and SAP packets have been disabled (the default), the following screen will be displayed:

```
IPX extended RIPs and SAPs off
```

If extended RIP and SAP packets have been enabled, the following screen will be displayed:

```
IPX extended RIPs and SAPs on
```

ipx timer

Command Usage

Adjust the time between RIP and SAP messages.

Syntax Options

ipx timer [*group-number***] <***rip-timer***> <***sap-timer***>**

Definitions:
group-number = specifies a group for which RIP and SAP timer values are to be adjusted (e.g., **4**)
rip-timer = specifies a RIP timer value (value must be between 1 and 180)
sap-timer = specifies a SAP timer value (value must be between 1 and 180)

♦ Syntax Note ♦
If you do not include a group number in the command line, the specified RIP and SAP timer values will be applied to *all* groups.

Command Examples:
ipx timer 4 180 60
ipx timer 60 30

Corresponding UI Command

ipxtimer

Remarks

The standard time between broadcasts of RIP and SAP messages is 60 seconds. This default may be modified in order to alleviate network congestion or to facilitate the discovery of network resources.

no ipx timer

Command Usage

Restore RIP and SAP timer values to the switch's default timer value of 60 seconds.

Syntax Options

no ipx timer [*group-number***]**

Definitions:
group-number = specifies a group for which RIP and SAP timer values will be restored to default (e.g., **4**)

♦ Syntax Note ♦

If you do not include a group number in the command line, RIP and SAP timer values will be restored to default on *all* groups.

Command Examples:
no ipx timer 77
no ipx timer

Corresponding UI Command

ipxtimer

view ipx timer

Command Usage

View current RIP and SAP timer values.

Syntax Options

view ipx timer (No additional syntax options are used.)

Corresponding UI Command

ipxtimer

Screen Output

If *no* user-defined RIP and SAP timer values have been set, the following screen will be displayed:

```
No timers to display.
```

If user-defined RIP and SAP timer values *have* been set, a screen similar to the following will be displayed:

A screen similar to the following displays:

```
 #     Group    RIP Timer (secs)   SAP Timer (secs)
===   ======   ================   ================
 1       1            30                 15
 2     global         45                 45
```

Table Description

Group. Displays the group number or **global** to indicate all groups.

RIP Timer (secs). Displays the RIP timer configured for the group using the **ipx timer** command.

SAP Timer (secs). Displays the SAP timer configured for the group using the **ipx timer** command.