



H3C MSR Router Series Comware 5 IPX Configuration Guide

New H3C Technologies Co., Ltd.
<http://www.h3c.com>

Software version: MSR-CMW520-R2516
Document version: 20180820-C-1.13

Copyright © 2006-2018, New H3C Technologies Co., Ltd. and its licensors

All rights reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of New H3C Technologies Co., Ltd.

Trademarks

H3C, **H3C**, H3CS, H3CIE, H3CNE, Aolynk, , H³Care, , IRF, NetPilot, Netflow, SecEngine, SecPath, SecCenter, SecBlade, Comware, ITCMM and HUASAN are trademarks of New H3C Technologies Co., Ltd.

All other trademarks that may be mentioned in this manual are the property of their respective owners.

Notice

The information in this document is subject to change without notice. All contents in this document, including statements, information, and recommendations, are believed to be accurate, but they are presented without warranty of any kind, express or implied. H3C shall not be liable for technical or editorial errors or omissions contained herein.

Preface

This configuration guide describes multicast fundamentals and configuration of IPX networks.

This preface includes the following topics about the documentation:

- [Audience.](#)
- [Conventions.](#)
- [Documentation feedback.](#)

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the routers.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x y ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x y ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x y ... }*	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x y ...]*	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the New User window opens; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
 TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Configuring IPX	1
Overview.....	1
IPX address structure.....	1
IPX RIP.....	1
IPX SAP.....	1
IPX NetBIOS.....	2
Protocol and standards.....	2
Hardware compatibility with IPX.....	2
Configuring basic IPX.....	2
Configuring IPX routing.....	3
Configuration prerequisite.....	3
Configuring an IPX static route.....	3
Configuring IPX route number limitation.....	4
Redistribute active static routes into RIP.....	4
Configuring IPX RIP parameters.....	4
Configuring IPX SAP.....	5
Configuration prerequisite.....	5
Enabling IPX SAP.....	5
Configuring IPX SAP timers.....	5
Configuring a response mode for IPX SAP GNS request.....	6
Configuring IPX service information.....	6
Configuring the IPX forwarding feature.....	7
Configuration prerequisites.....	7
Configuring IPX forwarding feature.....	7
Pinging an IPX network.....	8
Configuration prerequisites.....	8
Configuration procedure.....	8
Displaying and maintaining IPX configuration.....	8
IPX configuration example.....	9
Troubleshooting IPX configuration.....	10
Troubleshooting IPX forwarding failure.....	10
Troubleshooting IPX RIP.....	11
Troubleshooting IPX SAP.....	11
Troubleshooting IPX routing management.....	13
Index.....	14

Configuring IPX

Overview

Internetwork packet exchange (IPX) is a network layer protocol of NetWare. Its position in NetWare is similar to IP in TCP/IP. IPX implements such functions as address filling, routing, and packet forwarding.

IPX is a connectionless protocol. Though both data and the destination IPX address are included in an IPX packet, IPX does not confirm whether the packet is forwarded successfully. Such functions as confirmation of forwarding success and connection control are provided by the protocol at the layer above IPX. Any IPX packet is considered an independent entity that is not related to any other IPX packets logically or sequentially.

IPX address structure

The IPX address structure differs from IP. An IPX address consists of the network address and node address, in the format: network.node.

The network address, with a length of 4 bytes and expressed by an 8-digit hexadecimal, identifies the physical network where the site lies.

The node address identifies a node in the network, has the same structure as MAC address, and has a length of 6 bytes. It is input as three parts of 2-byte digits separated by - and it cannot be a broadcast or multicast address.

For example, in the IPX address bc.0-cb-47, the network address is bc (more accurately, it is 000000bc) and the node address is 0-cb-47 (more accurately, it is 0000-00cb-0047). Therefore, an IPX address can also be expressed in the form of N.H-H-H, in which N is the network address and H-H-H is the node address.

IPX RIP

IPX employs routing information protocol (RIP) to maintain and advertise dynamic routing information.

Through RIP, an IPX router exchanges routing information with neighbors and maintains an inter-network routing information database (usually called "routing table") according to network changes. When the router receives a packet, it finds a next hop from the routing table to forward the packet.

IPX SAP

Service advertising protocol (SAP) is used to advertise the service types that servers provide and their addresses. IPX advertises dynamic service information through SAP. When a server starts, it broadcasts services it can provide through SAP. When being shut down, the server informs clients of the termination of services through SAP.

Through SAP, an IPX router creates and maintains an inter-network service information database (usually called "service information table"). A server on the same network periodically broadcasts its service types and address. Clients not on the same network as the server cannot get such information directly, which is collected by the SAP proxy and saved in the server information table in the IPX router for advertisement to such clients. Because server information is dynamically updated by SAP, clients can always obtain latest server information.

SAP defines three types of packets, service query, service response, and periodic updates. The following subsections describe how SAP operates:

NetWare client initialization

When a NetWare client is initializing, it needs to locate a server. To do so, the client broadcasts a get nearest server (GNS) request. At least one router or server can give a SAP response, which contains information such as packet type, service type, and server name and address. The NetWare client can communicate with the server through the IPX address in the response packet.

Because the GNS request is broadcast, the client can only get a response from the server in the local IPX network.

To locate a server in another network, the IPX router can send a RIP request to get the route to the server, and send the route and service information to the client. In this way, the client can communicate with a server in another network.

Periodic update of SAP

A server broadcasts a SAP packet to provide the service name and type, and its IPX address. The IPX router that receives the broadcast will add the service to the service information database and periodically broadcast such information in the directly connected networks. The advertisements can thus flood the entire network.

By default, SAP broadcasts are sent every 60 seconds. Each packet can have up to seven service information items by default. If a large amount of service information needs to broadcast, the information can be sent in several packets. For example, 20 service information items can be sent in three packets.

IPX NetBIOS

As a broadcast, a NetBIOS packet is not routable. Therefore, a certain mechanism is needed for the routing device to forward such packets.

To enable use of network basic input/output system (NetBIOS) in a NetWare environment, Novell uses a mechanism to set the packet type contained in the IPX header to 20, indicating that the IPX packet is a NetBIOS packet. A device must forward such packets according to certain rules to make sure NetBIOS packets are transmitted in the IPX network.

Protocol and standards

- RFC 1132, *Standard for the transmission of 802.2 packets over IPX networks*
- RFC 1634, *Novell IPX Over Various WAN Media (IPXWAN)*

Hardware compatibility with IPX

IPX is not available on the following routers:

- MSR 2600.
- MSR 30-11.
- MSR 30-11E.
- MSR 30-11F.
- MSR3600-51F.

Configuring basic IPX

Follow these guidelines when you configure basic IPX:

- The node address specified with the **ipx enable [node node]** command is the global node address, used by all interfaces but the Ethernet interfaces on the router. If no node address is specified, the router specifies the MAC of the first Ethernet interface as the global node address. If no Ethernet interfaces are available, the router generates the global node address randomly according to the system clock. An Ethernet interface uses its own MAC address as the node address rather than the global one.
- A VLAN interface uses its own MAC address as the node address. You need not specify a node address when enabling IPX.
- An interface can only have one network number. If the IPX network number of an interface is deleted, its IPX configuration and static routing information are also deleted.

To configure basic IPX:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Enable IPX protocol.	ipx enable [node node]	Disabled by default.
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Configure an IPX network number for the interface.	ipx network <i>network-number</i>	By default, no network number is specified for the interface—IPX is still disabled on the interface even IPX is enabled in system view.

Configuring IPX routing

With the IPX protocol enabled on an interface, the system will automatically enable RIP to maintain and advertise dynamic routing information. Configure the following routing features based on the actual network requirements:

- Configuring IPX static routes
- Configuring IPX route number limit
- Configuring IPX RIP static route redistribution
- Configuring IPX RIP related parameters

Configuration prerequisite

Configure basic IPX.

Configuring an IPX static route

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Configure an IPX static route.	ipx route-static <i>dest-network</i> { <i>network.node</i> <i>interface-type</i> <i>interface-number</i> } [preference <i>value</i>] [tick <i>ticks</i> hop <i>hops</i>]	The IPX static route with a network number of 0xFFFFFFFFE is the default route. The interface specified by <i>interface-type interface-number</i> can only be a PPP interface.

Configuring IPX route number limitation

In IPX, the maximum number of static and dynamic routes to the same destination address permitted in the routing table can be configured. The number of equivalent routes for load balancing can also be configured. The two configurations have no direct relation, so changing one of the configurations will not affect the other.

When the number of dynamic and static routes to the same destination reaches the upper limit, newly found dynamic routes will be discarded instead of being added to the routing table. If the newly configured maximum value is smaller than the previous one, the excessive routes will not be deleted until they get aged out or until they are deleted manually.

If the number of equivalent load balanced routes is less than the number of active routes, the system will turn the excessive active routes into inactive routes; if the number of newly configured equivalent routes is bigger than the number of active routes, and equivalent inactive routes exist, the system will change these inactive routes to active ones to reach the number of configured equivalent load balanced routes.

To configure IPX route number limitation:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Configure the maximum number of routes to the same destination.	ipx route max-reserve-path <i>paths</i>	Optional. The default is 4.
3. Configure the maximum number of equal cost routes for load balancing.	ipx route load-balance-path <i>paths</i>	Optional. The default is 1.

Redistribute active static routes into RIP

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Redistribute active static routes into RIP.	ipx rip import-route static	Disabled by default.

Configuring IPX RIP parameters

The IPX RIP update interval must be identical on all routers in the network to keep consistency of routing tables.

If a route entry is not updated within the aging interval, it is removed from the routing table and the associated dynamic service information entry is also removed.

To configure IPX RIP parameters:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Specify an IPX RIP update interval.	ipx rip timer update <i>seconds</i>	Optional. The default is 60 seconds.
3. Configure an aging interval for IPX RIP routing entries.	ipx rip multiplier <i>multiplier</i>	Optional. The default is 3 times the update interval.

Step	Command	Remark
4. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
5. Configure the maximum length of IPX RIP updates.	ipx rip mtu <i>bytes</i>	Optional. The default is 432 bytes.

Configuring IPX SAP

With IPX enabled on an interface, the system will automatically use SAP to maintain and advertise dynamic service information. You can also configure the SAP related parameters or service information based on actual network requirements.

Configuration prerequisite

Configure basic IPX.

Enabling IPX SAP

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable IPX SAP.	undo ipx sap disable	Optional. By default, IPX SAP is enabled after IPX is enabled on the interface.

Configuring IPX SAP timers

In a large network, IPX SAP broadcasts might occupy much bandwidth. Changing IPX SAP update interval is an effective way to reduce bandwidth occupation. Configure IPX SAP aging interval as a value multiple times the update interval.

All servers and routers on the network must have the same SAP update interval. Otherwise, a router might consider a working server failed.

If the service information is not updated within the aging interval, it is be deleted from the service information table.

To configure IPX SAP timers:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Specify an IPX SAP update interval.	ipx sap timer update <i>seconds</i>	Optional. The default is 60 seconds.
3. Specify an aging interval for IPX SAP service information entries.	ipx sap multiplier <i>multiplier</i>	Optional. The default is 3 times the update interval.
4. Enter interface view.	interface <i>interface-type</i>	N/A

Step	Command	Remark
	<i>interface-number</i>	
5. Configure the maximum length of IPX RIP updates.	ipx sap mtu <i>bytes</i>	Optional. The default is 480 bytes—seven 64-byte service information items can be included in a SAP update.

Configuring a response mode for IPX SAP GNS request

GNS is a SAP message, broadcast by a SAP-enabled NetWare client. A NetWare server will respond to the request with a Give Nearest Server message.

If the NetWare server and the client reside in a common network, the server will respond to the client. If no NetWare server is available on the client's network, the connected router will respond.

You can configure a router to respond to a SAP GNS request with:

- The nearest server information. The nearest server has the least hops in the service information table.
- Round-Robin mode. All available servers in turn.

To configure a response mode for IPX SAP GNS request:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Configure the router to respond to a request.	<ul style="list-style-type: none"> • In Round-robin mode: ipx sap gns-load-balance • With the nearest server: undo ipx sap gns-load-balance 	Optional. By default, the round-robin mode is used.
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable the interface to respond to GNS requests.	undo ipx sap gns-disable-reply	Optional. Enabled by default.

Configuring IPX service information

Typically, a client only uses the service advertised by NetWare server and saved by the advising router. In order that the client can always use a specific service, static service information can be manually added to the service information table.

An IPX router supports up to 10,240 service information items, 2,048 service types, and 5,120 static service information items (including all service types). You can configure the maximum service information items for a certain type of service.

If the route associated with a static service information item is invalid or deleted, the static service information item will be prevented from broadcast, until the router finds a new valid route associated with service information.

The maximum queue length of the same service type items does not limit the amount of static service information but the amount of dynamic service information. If the newly configured queue length is less than the original length, the table items in the service information table will not be deleted; if the amount of service information for the same service type reaches the configured value, new service information items will not be added.

To configure IPX service information:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Add an IPX static service information item.	ipx service <i>service-type server-name network.node socket</i> hop <i>hopcount</i> [preference <i>preference</i>]	N/A
3. Configure the maximum queue length of the same service type items.	ipx sap max-reserve-servers <i>length</i>	Optional. 2048 by default.

The following table gives values of some service types:

Service type	Value
Unknown	0000h
Print Queue	0003h
File Server	0004h
Job Server	0005h
Print Server	0007h
Archive Server	0009h
Remote Bridge Server	0024h
Advertising Print Server	0047h
Reserved	Up To 8000h
Wildcard	FFFFh (-1)

Configuring the IPX forwarding feature

Configuration prerequisites

Configure basic IPX.

Configuring IPX forwarding feature

IPX RIP and SAP periodically broadcast updating packets. With the triggered updating feature enabled, updating packets will be sent only upon route or service information changes, and flooding of broadcasts can be avoided.

Split horizon can avoid routing loops—routing information received from an interface is not permitted to be sent from the interface. In some cases, split horizon must be prohibited to ensure correct routing information transmission. In addition, split horizon prohibition does not take effect on point-to-point links.

The type 20 IPX packet is used in NetBIOS. You can either prohibit or permit the forwarding of type 20 broadcast packets based on the actual requirements.

To configure IPX triggered updating feature:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the IPX triggered update feature.	ipx update-change-only	Disabled by default.
4. Enable the IPX split horizon feature.	ipx split-horizon	Optional. Enabled by default.
5. Configure the encapsulation format of IPX frames.	ipx encapsulation [dot2 dot3 ethernet-2 snap]	Optional. The default is Ethernet_802.3 (dot3).
6. Configure an IPX forwarding delay.	ipx tick <i>ticks</i>	Optional. By default, 1 tick for Ethernet interfaces and VLAN interfaces, 30 ticks for asynchronous serial ports, 6 ticks for synchronous ports, with each tick roughly being 1/18 second.
7. Enable the forwarding of type 20 packets.	ipx netbios-propagation	Disabled by default.

Pinging an IPX network

Configuration prerequisites

Configure basic IPX.

Configuration procedure

To ping an IPX network:

Task	Command	Remark
Ping an IPX network to check connectivity.	ping ipx <i>network.node</i> [-c <i>count</i> -s <i>size</i> -t <i>timeout</i>] *	Available in any view.

Displaying and maintaining IPX configuration

Task	Command	Remark
Display IPX interface information.	display ipx interface [<i>interface-type</i> <i>interface-number</i>] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display IPX packets statistics.	display ipx statistics [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the active IPX routing information.	display ipx routing-table [<i>network</i>] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display detailed IPX	display ipx routing-table [<i>network</i>] verbose [[Available in any view.

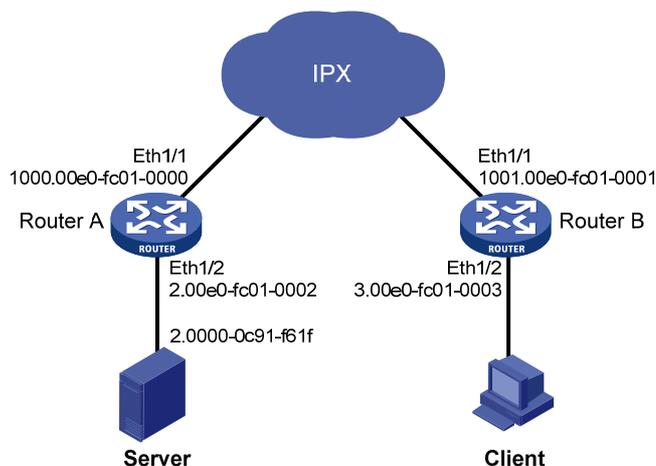
Task	Command	Remark
routing information (both active and inactive).	{ begin exclude include } <i>regular-expression</i>]	
Display IPX routing information for the specified route type.	display ipx routing-table protocol { default direct rip static } [inactive verbose] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display IPX routing statistics.	display ipx routing-table statistics [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the IPX service information table.	display ipx service-table [inactive name name network network order { network type } type service-type] [verbose] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Clear IPX statistics.	reset ipx statistics	Available in user view.
Clear IPX routing information.	reset ipx routing-table statistics protocol { all default direct rip static }	Available in user view.

IPX configuration example

Network requirements

- Router A and Router B are connected through an IPX network. The IPX address of Ethernet 1/1 on Router A is 1000.00e0-fc01-0000 and that on Router B is 1001.00e0-fc01-0001.
- The server is installed with NetWare 4.1 and its IPX address is 2.0000-0c91-f61f, packet encapsulation format is Ethernet_II. The client is a PC. Its network ID is 3, and packet encapsulation format is SNAP.
- The server provides file and printing services. The client can access these services through the IPX network.

Figure 1 Network diagram



Configuration procedure

1. Configure Router A:


```
# Enable IPX.
<RouterA> system-view
[RouterA] ipx enable
# Enable IPX on the interface Ethernet 1/2, with the network ID being 2.
```

```
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] ipx network 2
# Set the packet encapsulation format on the Ethernet interface to Ethernet_II.
[RouterA-Ethernet1/2] ipx encapsulation ethernet-2
[RouterA-Ethernet1/2] quit
# Enable IPX on the interface Ethernet 1/1, with the network ID being 1000.
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] ipx network 1000
[RouterA-Ethernet1/1] quit
```

2. Configure Router B:

```
# Enable IPX.
<RouterB> system-view
[RouterB] ipx enable
# Enable IPX on the interface Ethernet 1/2, with the network ID being 3.
[RouterB] interface ethernet 1/2
[RouterB-Ethernet1/2] ipx network 3
# Set the packet encapsulation format on the Ethernet interface to Ethernet_SNAP.
[RouterB-Ethernet1/2] ipx encapsulation snap
[RouterB-Ethernet1/2] quit
# Enable IPX on the interface Ethernet 1/1, with the network ID being 1001.
[RouterB] interface ethernet 1/1
[RouterB-Ethernet1/1] ipx network 1001
[RouterB-Ethernet1/1] quit
# Configure a Server file service information item.
[RouterB] ipx service 4 server 2.0000-0c91-f61f 451 hop 2
# Configure a Server print service information item.
[RouterB] ipx service 26B tree 2.0000-0c91-f61f 5 hop 2
```

RIP and SAP are automatically enabled when the **ipx network** command is issued on an IPX interface. Therefore, in this example, no routing protocol is configured.

Troubleshooting IPX configuration

Troubleshooting IPX forwarding failure

IPX cannot go up on a PPP link

- Confirm whether network IDs of both ends of the link are the same. Reconfigure them if they are different.
- Confirm whether node IDs of both ends of the link are different. Reconfigure them if they are the same.

Failed to ping a destination address

- Confirm whether the destination address is correct.
- Use the **display ipx interface** command to check the interface configuration. The network ID and IPX frame encapsulation format on the directly connected interfaces must be the same.
- Use the **display ipx routing-table** command to display routing information. Check whether a route to the destination network is available.

- Enable IPX packet debugging using the **debugging ipx packet** command. According to the detailed information displayed about IPX packets received, transmitted, forwarded, and discarded, you can locate the error.

Packets are discarded

If IPX packet debugging information displays that a packet is discarded, and the information displayed is **Packet size is greater than interface MTU!**, it indicates that the output packet size is greater than the maximum packet size that the interface can transmit. Use the **display interface** command to check the interface MTU and use the **display ipx interface** command to check the RIP and SAP packet size. If RIP or SAP packet size is greater than interface MTU, RIP or SAP packet cannot be sent out this interface.

SAP packets cannot be received

Use the **display ipx interface** command to check the receiving interface configuration. If SAP is disabled on this interface, SAP packets from this interface will be discarded.

IPX type 20 packets cannot be transmitted to any other network segment

- Use the **display ipx interface** command to check whether the forwarding for IPX type 20 packets is enabled on the receive/send interfaces. If it is not enabled, IPX type 20 packets cannot be forwarded.
- Enable IPX packet debugging using the **debugging ipx packet** command. If the debugging information displays that the type 20 packet is discarded and the prompt is **Transport Control field of IPX type-20 packet >= 8!**, it indicates the IPX type 20 packet can only be forwarded 8 times. If the upper limit is reached, the IPX type 20 packet will not be forwarded further.

Troubleshooting IPX RIP

No routes can be learned from a peer

- Enable IPX RIP debugging using the **debugging ipx rip packet verbose** command. Check whether RIP packets can be received from the peer. If not, problems on the lower layer connection of the two devices might exist.
- If a RIP packet with routing information is received from the peer, use the **debugging ipx rip event** command to see whether the received route is added to the routing table. If not, faults occurred when the route was added to the routing table. Possible faults could be that the packet encapsulation formats of the end interfaces do not match, or a bad RIP packet is received and discarded.

A static route is redistributed to IPX RIP but no static route is advertised

- Use the **display ipx routing-table** command to check whether the static route exists.
- If the static route is not available, use the **display ipx routing-table verbose** command to check whether it is inactive. If so, check further why it is inactive. Possible reasons could be: the next hop network ID is unreachable, or the outgoing interface is down. When the route becomes active, it can be advertised as a RIP route.
- If the static route exists in the routing table, check its hops. If hops are more than or equal to 15, the static route cannot be advertised.

Troubleshooting IPX SAP

Unable to add a static service information item to SIT

- Use the **display ipx service-table inactive** command to see whether the item is inactive. If so, it indicates that no active route to the destination server exists.

- Use the **display ipx service-table** command to see whether the service information items reach the upper limit. IPX supports up to 10240 service information items, 2048 service types and 5120 static service items.

No active service information item in SIT

- Use the **display ipx service-table inactive** command to check whether the service information item is inactive. If so, it indicates that no active route to the destination server exists.
- Use the **display ipx interface** command to verify that the interface is UP and SAP is enabled.
- Use the **display ipx routing-table** command to verify that the active route to the server has a hop number less than 16.
- Another possible reason is that no sufficient memory is available to add the service information item to the SIT. You can remove some static service information items.

No new dynamic service information items in SIT

- Use the **debugging ipx packet** and **debugging ipx sap packet verbose** commands to check whether relevant packets are received. If no packet is received, problems in lower layer network connection might exist.
- If IPX is disabled, use the **ipx enable** command in system view to enable IPX.
- Use the **display ipx interface** command to make sure IPX is configured on relevant interfaces.
- If SAP is disabled, use the **undo ipx sap disable** command to enable SAP.
- Check whether the number of SAP service information items reaches the upper limit. The IPX implementation supports up to 10240 service information items and 2048 service types.
- The MTU of SAP should be less than that of the physical layer.

No updates are received on an interface

- Use the **debugging ipx packet** and **debugging ipx sap packet verbose** commands to check packet contents. All incoming and outgoing packets are displayed in debugging information. If no related packets are displayed, problems in lower layer network connection might exist.
- Use the **display ipx interface** command to make sure SAP is enabled on the interface.
- Make sure the active route to the server has a hop number less than 16.
- Use the **display current-configuration** command to check whether the updating interval is too long.

No updates sent out an interface

- Use the **debugging ipx packet** and **debugging ipx sap packet verbose** commands to check packet contents. If such update packets are displayed in debugging information, possibly the SAP MTU is larger than the interface MTU. Hence, the packets are discarded by the lower layer.
- Use the **display ipx interface** command to check whether the interface is enabled with triggered update. If so, the interface will not periodically broadcast update packets.
- If no SAP packets are sent out the interface, check whether all service information is learned from the interface. If so, split horizon might be the reason that no service information is sent out the interface.

SAP does not respond to GNS requests

- Use the **debugging ipx sap packet** command to check whether GNS request packets are received.
- Make sure SAP is enabled on the receiving interface.
- Use the **display ipx interface** command to check whether the interface is disabled from responding to GNS requests. If so, use the **undo ipx sap gns-disable-reply** command to enable the interface.

- Use the **display ipx service-table** command to check whether the requested service information is available in the SIT table. If not, SAP will not respond.
- If the requested service information is available, check whether the service information is learned from the interface that received the GNS requests. In that case SAP will also not respond to the GNS requests.

SAP does not respond to GNS requests in the Round-robin mode

- Use the **display current-configuration** command to make sure Round-robin is configured.
- If Round-robin is configured, verify whether multiple equivalent service information items exist for the service type of the requests. The equivalent service information items must have the same RIP ticks, RIP hops, SAP hops and SAP preference.

Troubleshooting IPX routing management

No dynamic routing protocols are configured on the device

The physical status and link layer protocol are both UP on an interface, but IPX packets cannot be forwarded correctly:

- Use the **display ipx routing-table protocol static** command to check whether a correct static route is configured.
- Use the **display ipx routing-table** command to verify the static route takes effect, and to check whether the next hop address is not specified or not correct on the non PPP interface.

Routes received from a neighbor router cannot be found by using the display ipx routing-table verbose command

- Use the **display current-configuration** command to check whether the maximum dynamic route number is configured on a per network ID basis, with the command **ipx route max-reserve-path**. If it is not configured, the default value 4 is used.
- Use the **display ipx routing-table verbose** command to check whether the existing dynamic route number under the destination network ID has reached the maximum number.
- If the upper limit is reached, the newly received routes will not be added to the routing table. You can use the **ipx route max-reserve-path** command to adjust the maximum number of dynamic routes.

Index

C D H I O P T

C

Configuring basic IPX, [2](#)

Configuring IPX routing, [3](#)

Configuring IPX SAP, [5](#)

Configuring the IPX forwarding feature, [7](#)

D

Displaying and maintaining IPX configuration, [8](#)

H

Hardware compatibility with IPX, [2](#)

I

IPX configuration example, [9](#)

O

Overview, [1](#)

P

Pinging an IPX network, [8](#)

T

Troubleshooting IPX configuration, [10](#)