

NOKIA

Interfaces configuration in Voyager for IPSO 3.8NET

The product described in this document is still under development by Nokia Networks. However, in the interest of offering early possibility to our customers to evaluate the documentation, this documentation is provided in draft form. Therefore the customer understands that the information in this document is subject to change without notice and describes only the prototype product defined in the introduction of this documentation in its current state of development. Nokia Networks welcomes customer comments as part of the process of continuous development and improvement of its products and the documentation.

This document is not a final customer document and Nokia Networks does not take responsibility for any errors or omissions in this document. No part of it may be reproduced or transmitted in any form or means without the prior written permission of Nokia Networks. The document has been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using it.

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between Nokia Networks and the customer.

Nokia Networks WILL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT OR FOR ANY DAMAGES, INCIDENTAL OR CONSEQUENTIAL (INCLUDING MONETARY LOSSES), that might arise from the use of this document or the information in it. UNDER NO CIRCUMSTANCES SHALL NOKIA BE RESPONSIBLE FOR ANY LOSS OF USE, DATA, OR INCOME, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY OR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES HOWSOEVER CAUSED.

THE CONTENTS OF THIS DOCUMENT ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE MANDATORY LAW, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS DOCUMENT. NOKIA RESERVES THE RIGHT TO REVISE THIS DOCUMENT OR WITHDRAW IT AT ANY TIME WITHOUT PRIOR NOTICE.

This document and the product it describes are protected by copyright according to the applicable laws.

NOKIA and Nokia Connecting People are registered trademarks of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective companies, and they are mentioned for identification purposes only.

Copyright © Nokia Corporation 2003. All rights reserved. Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of Nokia is prohibited.

Contents

	Contents	3
1	Overview of interface configuration	5
2	Virtual LAN interfaces	13
3	Unnumbered interfaces	15
4	Configuring physical Ethernet interfaces	17
5	Configuring logical Ethernet and VLAN interfaces	21
6	Ethernet interface configuration example	23
7	Gigabit Ethernet interface configuration example	27
8	Creating VLAN interfaces	31
9	Deleting logical interfaces	33
10	Configuring physical ATM interfaces	35
11	Creating logical ATM interfaces	37
12	ATM point-to-point interface configuration example	39
13	IP over ATM configuration example	43
14	Configuring physical serial interfaces	47
15	Configuring ATM point-to-point interfaces	49
16	Configuring ATM LIS interfaces	53
17	Serial interface configuration example	55
18	Configuring Cisco HDLC protocol	59
19	Configuring physical T1 interfaces	63
20	T1 interface configuration example	67
21	Configuring physical E1 interfaces	71
22	Managing unnumbered interfaces	75
23	Configuring a static route over an unnumbered interface	79

24	Configuring OSPF over an unnumbered interface	81
25	Configuring PPP protocol	83
26	Configuring frame relay protocol	87
27	Configuring loopback interfaces	91
28	Creating tunnels	93
29	Configuring tunnels	95
30	GRE tunnel configuration example	99
31	HA GRE tunnel configuration example	101
32	DVMRP tunnel configuration example	105
33	Configuring ARP	109
34	Creating static ARP entries	111
35	Creating proxy ARP entries	113
36	Viewing dynamic ARP entries	115
37	Removing ARP entries	117
38	Configuring ARP for ATM interfaces	119
39	Creating static ATM ARP entries	121
40	Removing ATM ARP entries	123

1

Overview of interface configuration

This section describes how to configure network devices and assign IP addresses to them using Voyager.

Note

If you have local interfaces on a general purpose line card (GPLC), you must first select the line card by clicking the *Line Card Configuration* link on the *Configuration* page, click the name of the line card, and then click the *Interfaces* link. See *Making configuration changes to general purpose line cards*.

Interface types

Nokia NAPs support the following interface types.

Note

Consult the appropriate hardware installation guide to find out what interfaces your unit supports.

- Ethernet/Fast Ethernet/Gigabit Ethernet
- ATM (RFC1483 PVCs only)
- Serial (V.35 and X.21) running PPP, point-to-point Frame Relay, or Cisco HDLC
- T1/E1 running PPP, Frame Relay, or Cisco HDLC
- GRE Tunneling
- Unnumbered Interface

You can configure these interfaces with IP addresses. You also can assign additional IP addresses to the loopback and Ethernet interfaces. All interface types support IP multicast.

Network interfaces

Voyager displays network interfaces as physical interfaces. A physical interface exists for each physical port on a network interface card (NIC) and onboard interfaces installed in the unit. Physical interface names have the form:

IP3400: **<type>-s<GPLC slot #>/s<CPCI slot #>p<port#>**

IP740: **<type>-s<slot #> p<port#>**

The following describes interface variable names:

<type> is a prefix indicating the family device type. The interface-name prefixes for each type are as follows:

Type	Prefix	Remarks
Ethernet	eth	Supported in IP3400 and IP740
ATM	atm	Supported in IP3400 and IP740
Serial (X.21 or V.35)	ser	Supported only in IP740
T1/E1	ser	Supported in IP3400 and IP740

<GPLC slot #> is the slot number of the GPLC.

<CPCI slot #> is the slot number of the CPCI in the GPLC.

<slot #> is the slot number of the CPCI.

<port #> is the physical port number of the interfaces in CPCI. The first port on a NIC is port one. For example, a four-port Ethernet NIC in CPCI slot 1 of the GPLC slot 2 is represented by four physical interfaces:

eth-s2/s1p1, eth-s2/s1p2, eth-s2/s1p3, and eth-s2/s1p4.

The loopback interface also has a physical interface named **loop0**.

Use Voyager to set the attributes of the device. For example, line speed and duplex mode are attributes of an Ethernet physical interface. Each communications port has exactly one physical interface.

IP addresses

On any physical Interface you must create logical interface(s) to assign IP address for the interface and then add the proper destination address or network address.

For ATM devices, you create a new logical interface each time you configure an RFC1483 PVC for the device. Serial and T1/E1 devices have one logical interface when they are running PPP or Cisco HDLC. Serial and T1/E1 devices running point-to-point Frame Relay have a logical interface for each PVC configured on the port. You also have the option of configuring an unnumbered interface for point-to-point interfaces. Tunnels, however, cannot be configured as unnumbered interfaces.

Logical interfaces, by default, are named after the physical interface for which they are created. If you wish, you can override this default name with a more descriptive or familiar name. Default logical interface names have the form:

IP3400: <type>-s<GPLC slot #>/s<CPCI slot #> p<port #> c<chan #>

IP740: <type>-s<slot #> p<port #> c<chan #>

onboard: <type> -p<port #> c-<chan>

The following describes interface variable names:

<type> is a prefix indicating the family device type.

<GPLC slot #> is the slot number of the GPLC.

<CPCI slot #> is the slot number of the CPCI in the GPLC.

<slot #> is the slot number of the CPCI.

<port #> is the physical port number of the interfaces in CPCI.

<chan #> is the channel number of the logical interface. For logical interfaces created automatically, the channel number is always zero. For logical interfaces created manually, the channel number is the identifier of the virtual circuit (VC) for which the interface is created (for example, the ATM VCI or the Frame Relay DLCI).

<i>Physical interface</i>	<i>Logical interface</i>			
	Default	Cisco HDLC	PPP	Frame Relay

Ethernet	One (c0)			
ATM	One per VCI (c#)			
Serial (X.21 or V.35)	One (c0)	One(c0)	Oneper DLCI (c#)	
T1/E1	One (c0)	One(c0)	Oneper DLCI (c#)	

For example, the logical interface of a physical interface **eth-s2p1** is called **eth-s2p1c0**. The logical interfaces for PVCs 17 and 24 on an ATM NIC in slot 3 are called **atm-s3p1c17** and **atm-s3p1c24** respectively. All interfaces have one logical interface per VLAN (Virtual LAN) ID.

Once a logical interface exists for a device, you can assign an IP address to it. For Ethernet, you must specify the interface's local IP address and the length (in bits) of the subnet mask for the subnet to which the device connects.

If you are running multiple subnets on the same physical network, you can configure additional addresses and subnet masks on the single logical interface connected to that network. You do not need to create additional logical interfaces to run multiple subnets on a single physical network.

For point-to-point media, such as ATM or serial, you can either assign IP addresses or configure an unnumbered interface. When assigning IP addresses you must specify the IP address of the local interface and the IP address of the remote system's point-to-point interface.

You can add only one local/destination IP address pair to a point-to-point logical interface. To assign IP addresses to multiple VCs, you must create a logical interface for each VC. IP subnets are not supported on point-to-point interfaces.

Whenever an unnumbered interface generates a packet, it uses the address of the interface that the user has specified as the source address of the IP packet. Thus, for a router to have an unnumbered interface, it must have at least one IP address assigned to it. The Nokia implementation of unnumbered interfaces does not support virtual links.

Indicators and interface status

The configuration and status of removable-interface devices are displayed. Interfaces can be changed while they are offline. The events, their effects, and indications are:

- If you hot-insert a device (not power down the unit first), it appears in the lists of interfaces immediately (after a page refresh) on the configuration pages.
- If you hot-pull a device, and no configuration exists for it, it disappears from the lists of interfaces immediately.
- If you hot-pull a device, and it had a configuration, its configuration details continue to be displayed and can be changed even after a reboot.
- Hotswapped interfaces that are fully seated in a router's chassis are represented in the ifTable (MIB-II), ipsoCardTable (NOKIA-IPSO-System-MIB), and the hrNetworkTable (Host-Resources-MIB).
- Unwanted configurations of absent devices can be deleted, which removes the physical and logical interfaces from all interface lists.
- None: If no color indication is displayed, the interface is disabled. To enable the interface, click on the physical interface name to go to its configuration page.
- Blue: The device corresponding to this interface has been removed from the system, but its configuration remains. To delete its configuration, click on the physical interface name to go to its configuration page.
- Red: The interface is enabled, but the device does not detect a connection to the network.
- Green: The interface is enabled, connected to the network and the physical link is up.

Note

The traffic will not go through unless the interface is configured with IP address.

Address resolution protocol (ARP)

ARP allows a host to find the physical address of a target host on the same physical network using only the target's IP address. ARP is a low-level protocol that hides the underlying network physical addressing and permits assignment of an arbitrary IP address to every machine. ARP is considered part of the physical network system and not as part of the internet protocols.

The loopback interface

By default, the loopback interface has 127.0.0.1 configured as its IP address. Locally originated packets sent to this interface are sent back to the originating process.

You might want to assign an address to the loopback interface that is the same as the OSPF ID, or is the termination point of a BGP session. This allows adjacencies to stay up even if the outbound interface is down. Do not specify an IP subnet mask length when you add addresses to the loopback interface.

Tunnel interfaces

Tunnel interfaces are used to encapsulate protocols inside IP packets. Use tunneling to send network protocols over IP networks that don't support them.

Create a tunnel logical interface by specifying an encapsulation type. Use Voyager to set the encapsulation type. Voyager supports two encapsulation types, DVMRP and GRE.

The tunnel logical interface name has the form: **tun0c<chan>**, where **<chan>** (channel number) is an instantiation identifier.

Distance vector multicast routing protocol (DVMRP) tunnels

DVMRP tunnels encapsulate multicast packets using IP-in-IP encapsulation. The encapsulated packets appear as unicast IP packets. This technique allows two multicast routers to exchange multicast packets even when they are separated by routers that cannot forward multicast packets. For each DVMRP tunnel you create, you must provide the IP address of the interface that forms the local endpoint of the tunnel and the IP address of the multicast router that is at the remote end of the tunnel forming the remote endpoint of the tunnel.

Note

The remote multicast router must support IP-in-IP encapsulation and must be configured with a tunnel interface to the local router.

When you have created the DVMRP tunnel interface, set all other DVMRP multicast configuration parameters from the DVMRP configuration page.

GRE tunnels

GRE tunnels encapsulate IP packets using generic routing encapsulation (GRE) without options. The encapsulated packets appear as unicast IP packets. For each GRE tunnel you create, you must assign a local and remote IP address. You also must provide the local and remote endpoint addresses of the interface to which this tunnel is bound. GRE tunnels provide redundant configuration between two sites for high availability. The remote router must also support GRE encapsulation and must be configured with a tunnel interface to the local router.

IP740 interface guidelines

The IP740 has four onboard Ethernet cards. The following table shows the interface conventions for the Ethernet cards:

<i>Physical</i>	<i>Logical</i>	<i>Type</i>
eth1	eth1c0	Ethernet/Fast Ethernet
eth2	eth21c0	Ethernet/Fast Ethernet
eth3	eth3c0	Ethernet/Fast Ethernet
eth4	eth4c0	Ethernet/Fast Ethernet

The IP740 is capable of accepting a maximum of 4 CPCI modules. The CPCI modules currently supported are 10/100, Gigabit Ethernet, ATM (OC-3), Viper Accelerator Card for encryption (uses the PCM slot), T1/E1, and X.21/V.35. The following table shows the CPCI module interface conventions, assuming that the CPCI module is in slot 1 of the NAP:

<i>CPCI Module</i>	<i>Physical</i>	<i>Logical</i>	<i>Type</i>
10/100	eth-s1p1	eth-s1p1c0	Ethernet/Fast Ethernet
	eth-s1p2	eth-s2p1c0	Ethernet/Fast Ethernet
	eth-s1p3	eth-s3p1c0	Ethernet/Fast Ethernet
	eth-s1p4	eth-s4p1c0	Ethernet/Fast Ethernet
ATM	atm-s1p1	atm-s1p1c0	ATM (point to point)
GigE	eth-s1p1	eth-s1p1c0	Gigabit Ethernet
X.21	ser-s1p1	ser-s1p1c0	Serial X.21
	ser-s1p2	ser-s1p2c0	
V.35	ser-s1p1	ser-s1p1c0	Serial V.35

	ser-s1p2	ser-s1p2c0	
T1	ser-s1p1	ser-s1p1c0	Serial RJ-48 T1
E1	ser-s1p1	ser-s1p1c0	Serial RJ-48 E1

IP3400 interface guidelines

The IP3400 supports 10/100 Ethernet, Gigabit Ethernet, and ATM (OC-3/SMF and MMF), and SS7. The following table shows the interface conventions for the IP3400:

	<i>On Board Ethernet</i>		<i>CPCI Slot 1</i>		<i>CPCI Slot 2</i>		<i>Remarks</i>
	<i>Physical</i>	<i>Logical</i>	<i>Physical</i>	<i>Logical</i>	<i>Physical</i>	<i>Logical</i>	
<i>CRP A</i>	eth1	eth1c0					Active CRP
<i>CRP B</i>							Standby CRP
<i>GPLC Slot 1</i>	eth-s1/1	eth-s1/1c0	eth-s1/s1p1 eth-s1/s1p2 eth-s1/s1p3 eth-s1/s1p4	eth-s1/s1p1c0 eth-s1/s1p2c0 eth-s1/s1p3c0 eth-s1/s1p4c0	eth-s1/s2p1 eth-s1/s2p2 eth-s1/s2p3 eth-s1/s2p4	eth-s1/s2p1c0 eth-s1/s2p2c0 eth-s1/s2p3c0 eth-s1/s2p4c0	For 10/100 CPCI module. The type will be either Ethernet or Fast Ethernet, depending on the speed.
<i>GPLC Slot 2</i>	eth-s2/1	eth-s2/1c0	eth-s2/s1p1	eth-s2/s1p1c0	No CPCI		The CPCI slot 1 has GigE.
<i>GPLC Slot 15</i>	eth-s15/1	eth-s15/1c0	atm-s15/s1p1	atm-s15/s1p1c0	atm-s15/s2p1	atm-s15/s2p1c0	Both CPCIs are ATM NICs.

2

Virtual LAN interfaces

Nokia supports virtual LAN (VLAN) interfaces on all supported ethernet interfaces. The use of VLAN interfaces lets you configure subnets with a secure private link to Check Point FW-1/VPN-1 with the existing topology. The use of VLAN enables the multiplexing of ethernet traffic into channels on a single cable.

The Nokia implementation supports adding a logical interface with a VLAN ID to a physical interface. In a VLAN packet, the OSI layer-two header, or MAC header, contains four more bytes than the typical ethernet header for a total of 18 bytes. When traffic arrives at the physical interface, the system examines it for the VLAN layer-two header and accepts and forwards the traffic if a VLAN logical interface is configured. If the traffic that arrives at the physical interface does not have a VLAN header, it is directed to the channel 0, or untagged, interface. In the Nokia implementation the untagged channel 0 interface drops VLAN packets sent to the subnets on that interface.

Outgoing traffic from a VLAN interface is tagged with the VLAN header. The Nokia appliance can receive and generate fully conformant IEEE 802.1Q tags. The IEEE802.1Q standard defines the technology for virtual bridged networks. The Nokia implementation is completely interoperable as a router, not as a switch.

VLAN example topology

The topology below represents a redundant router with load sharing and VLAN. Nokia appliance running Check Point FW-1 is configured with the virtual router redundancy protocol (VRRP). This protocol provides dynamic fail-over of IP addresses from one router to another in the event of failure. Each appliance is configured with Gigabit Ethernet and supports multiple VLANs on a single cable. The appliances receive and forward VLAN-tagged traffic to subnets configured for VLAN, creating a secure private network. In addition, the appliances are configured to create VLAN-tagged messages for output.

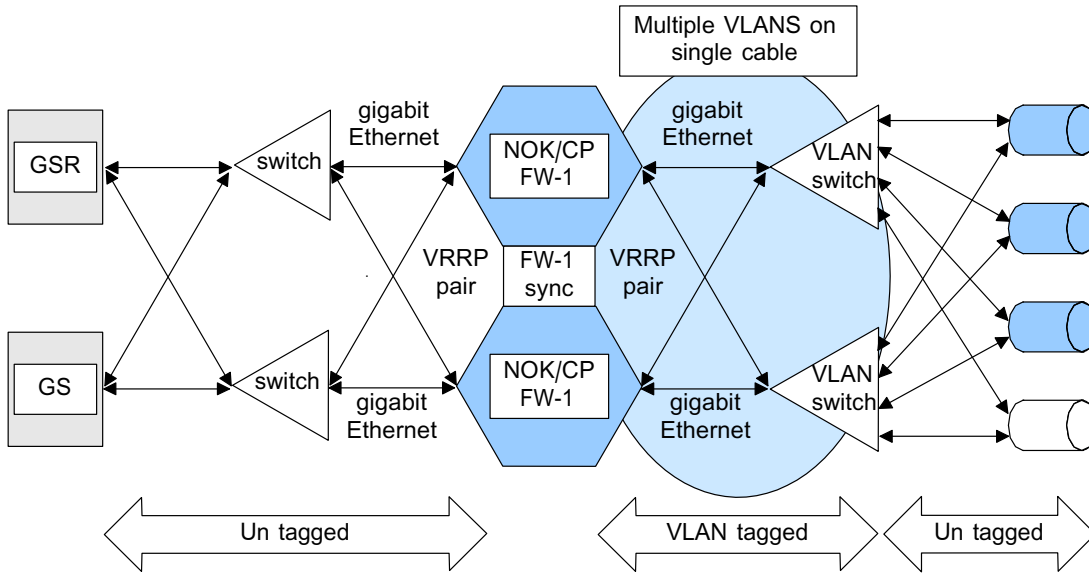


Figure 1. Fully redundant router with load sharing and VLAN

For more information, see *Creating VLAN interfaces* and *Configuring logical Ethernet and VLAN interfaces*

3

Unnumbered interfaces

Traditionally, each network interface on an IP host or router has its own IP address. This situation can cause inefficient use of the scarce IP address space because every point-to-point link must be allocated an IP network prefix. To solve this problem, a number of people have proposed and implemented the concept of unnumbered point-to-point lines. An unnumbered point-to-point line does not have any network prefix associated with it. As a consequence, the network interfaces connected to an unnumbered point-to-point line do not have IP addresses. Whenever the unnumbered interface generates a packet, it uses the address of the interface that the user has specified as the source address of the IP packet. Thus, for a router to have an unnumbered interface, it must have at least one IP address assigned to it.

The Nokia implementation of unnumbered interfaces supports OSPF (Open shortest path first) and static routes only. Virtual links are not supported.

Unnumbered interfaces and virtual links

The graphic below shows a network configuration that uses both virtual links and an unnumbered serial link. NAP A has two OSPF areas configured (Area 1 and Area 3), but it is not physically connected to the backbone area. Thus, a virtual link is configured between NAP A and NAP C. A virtual link is also configured between NAP B and NAP C because NAP B also is not physically connected to the backbone area. Both NAP B and NAP C are configured with IP addresses (10.10.10.2 and 101.10.10.1 respectively).

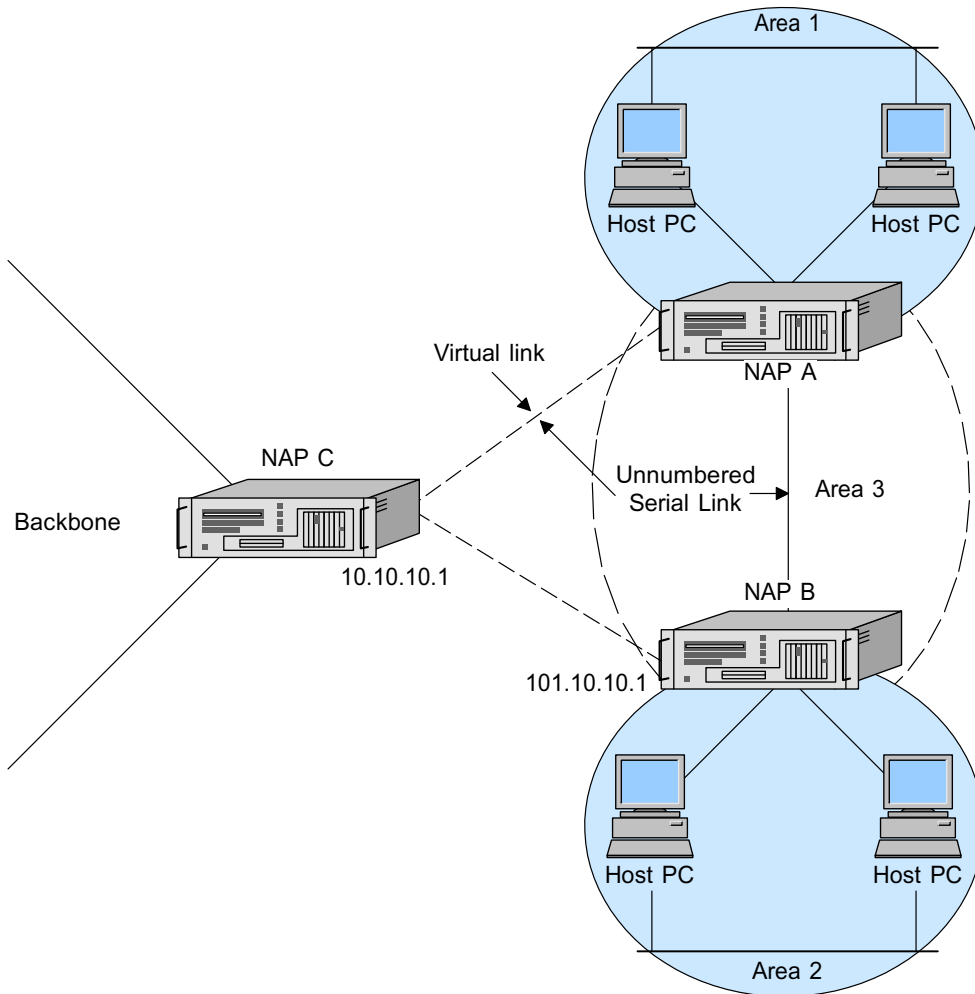


Figure 2. Network configuration using virtual links and an unnumbered serial link

The interfaces that comprise the virtual link between NAP A and NAP C are both configured as unnumbered. This link will fail because OSPF does not support a virtual link that uses an unnumbered interface on either end of the link. For more information, see *RFC 2328*.

Any virtual link that uses OSPF must have an IP address configured on both ends. The virtual link between NAP B and NAP C will function because each NAP is configured with an IP address.

For more information, see *Managing unnumbered interfaces*

4

Configuring physical Ethernet interfaces



Steps

1. **Go to the Interface Configuration page of the Voyager.**

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.

2. **Select the physical interface to configure.**

Click the physical interface link you want to configure in the **Physical** column. For example, click `eth-s2p1` or `eth-s2/s1p1`.

Expected outcome

The configuration page for the selected physical interface opens.

3. *If you are configuring an Ethernet or a Fast Ethernet interface*

Then

Select the link speed.

Click the **10 Mbit/Sec** or the **100 Mbit/Sec** radiobutton in the **Physical Configuration** table **Link Speed** field to select the link speed for the interface.

Note

This setting must be the same for all hosts on the network to which the device connects. Speed settings are only applicable for 10/100 Mbit/sec Ethernet interfaces.

4. *If you are configuring an Ethernet or a Fast Ethernet interface*

Then

Select the duplex mode.

Click the **Full** or **Half** radio button in the **Physical Configuration** table **Duplex** field to select the duplex mode.

Note

This setting must be the same for all hosts on the network to which the device connects. If the duplex setting of an Ethernet interface is incorrect, it may not receive data, or it may receive duplicates of the data it sends.

5. *If you are configuring an Ethernet or a Fast Ethernet interface*

Then

Enable or disable autoadvertising.

Click the **On** or the **Off** radio button in the **Physical Configuration** table **Autoadvertise** field to enable or disable the autoadvertise feature.

Further information

If autoadvertising is turned on, the device will advertise its configuration speed and duplex status using Ethernet negotiation.

6. *If you are configuring a Gigabit Ethernet interface*

Then

Enable or disable flow control.

Click the **On** or **Off** radio button in the **Physical Configuration** table's **Flow Control** field to select the appropriate choice. The default value is Off.

7. *If you are configuring a Gigabit Ethernet interface*

Then

Enable or disable Jumbo frame support.

Click the **On** or **Off** radio button in the **Physical Configuration** table's **Jumbo Frame** field to select the appropriate choice. The default value is Off.

Further information

When Jumbo frame support is enabled, you can define the MTU value for the logical interfaces of the device. The MTU value can be any number between 1500 and 1900.

8. Click Apply.

9. *If the logical interface has not been configured*

Then

Continue from Configuring logical Ethernet and VLAN interfaces.

Else

If you want to create new VLAN logical interfaces

Then

Continue from Creating VLAN interfaces.

- 10. To make your changes permanent, click Save.**

Further information

Note

For Gigabit Ethernet, the link speed and the duplex mode appear in the **Physical Configuration** table in the **Link Speed** field. The speed is fixed and the duplex mode is set to full at all times.

5

Configuring logical Ethernet and VLAN interfaces

Before you start

Note

Do not change the IP address you use in your browser to access Voyager, often called Management Interface. If you do, you can no longer access the network application platform (NAP) with your browser.

In order to configure a logical interface, you need to be on the configuration page of the logical interface:

1. Click **Config** on the Voyager home page.
2. Click the *Interfaces* link.
3. Click the logical interface link you want to configure in the **Logical** column.



Steps

1. *If you want to remove IP addresses*

Then

Select the IP addresses you want to delete.

Click the check box in the **Delete** column next to the IP addresses you want to delete. Click **Apply**.

2. *If you want to add an IP address*

Then

Enter the new IP address and mask length.

- a. Enter the IP address for the device in the **New IP Address** edit box.
 - b. Enter the length of the subnet mask in the **New Mask Length** edit box
3. *If you enabled jumbo frame support*

Then

Enter the MTU length (in bytes).

Enter a number in the IP MTU edit box to configure the maximum length (in bytes) of IP packets transmitted in this interface. The range of the MTU length for jumbo frames is 1500-1900.

Note

The MTU length must match the MTU length of the link partner. Packets longer than the MTU length will be fragmented before transmission.

4. Click Apply.**Expected outcome**

If you selected IP addresses to be deleted, the IP addresses disappear from the table.

If you entered a new IP address and subnet mask, each time you click **Apply** the configured IP address appears in the table. The entry fields remain blank to allow you to add more IP addresses.

5. To make your changes permanent, click Save.**Further information**

To add or remove more IP addresses, repeat the procedure.

For more information, see *Creating VLAN interfaces*, *Deleting logical interfaces*, *Ethernet interface configuration example* and *Gigabit Ethernet interface configuration example*

6 Ethernet interface configuration example

Purpose

This section describes how you might configure the interfaces of your network application platform (NAP) in an example network, using Voyager.

Before you start

Before you can configure the NAP using Voyager, you must configure an IP address on one of the interfaces. You can do this through the NAP console port during installation or by using the Lynx browser. This allows a graphical browser such as Microsoft Internet Explorer or Netscape Navigator to access the unit through that interface. You can use any graphical web browser to configure the other interfaces on the NAP by entering the IP address of the NAP in the location field of the browser.

The figure below shows the network configuration for this example.

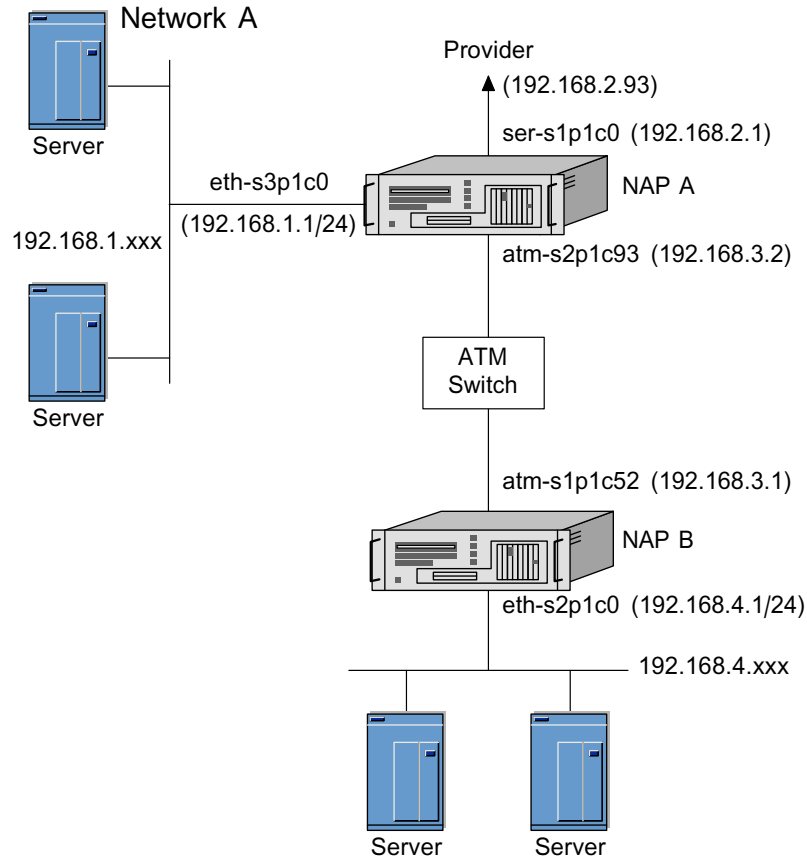


Figure 3. Example of network configuration for an Ethernet interface

In a company's main office, NAP A terminates a serial line to an Internet service provider, running PPP with a keep alive value of 10. NAP A also provides internet access Network A and a remote branch office connected via ATM PVC 93.

The branch office contains NAP B, which routes traffic between a local Fast Ethernet network and ATM PVC 52. It provides access to the main office and the Internet. We are configuring the Ethernet interface on NAP B.



Steps

1. Click **Config** on the home page.
2. Click the **Interfaces** link.
3. Click **eth-s2p1** in the **Physical** column of the table.

4. **Click the 100 Mbit/Sec radio button.**
5. **Click Apply.**
6. **Click `eth-s2p1c0` in the Logical Interfaces table to go to the *Interface* page.**
7. **Enter `192.168.4.1` in the New IP Address edit box.**
8. **Enter `24` in the New Mask Length edit box.**
9. **Click Apply.**
10. **Click the Up button to go the *Interfaces* page.**
11. **Click the On radio button for `eth-s2p1c0`.**
12. **Click Apply.**
13. **Click Save.**

7

Gigabit Ethernet interface configuration example

Purpose

This section describes how you might configure the interfaces of your network application platform (NAP) in an example network, using Voyager.

Before you start

Before you can configure the unit using Voyager, you must configure an IP address on one of the interfaces. You can do this through the unit's console port during installation or by using the Lynx browser. This allows a graphical browser such as Microsoft Internet Explorer or Netscape Navigator to access the unit through that interface. You can use any graphical web browser to configure the other interfaces on the NAP by entering the IP address of the NAP in the location field of the browser.

The figure below shows the network configuration for this example.

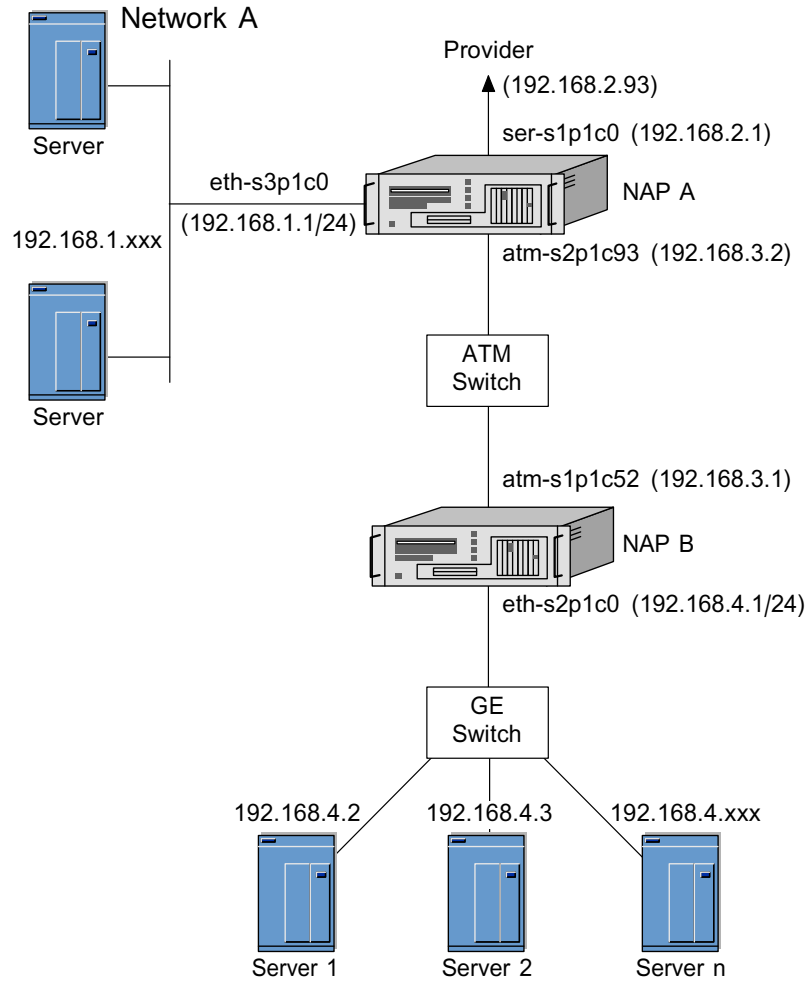


Figure 4. Example of network configuration for an Gigabit Ethernet interface

In a company's main office, NAP A terminates a serial line to an Internet service provider. NAP A also provides internet access for Network A and a remote branch office connected via ATM.

The branch office contains NAP B, which routes traffic between a local Gigabit Ethernet network and ATM. It provides access to the main office and the Internet. We are configuring the Gigabit Ethernet interface on NAP B.



Steps

1. Click **Config** on the home page.

2. Click the *Interfaces* link.
3. Click `eth-s2p1` in the Physical column of the table.
4. Click the On or Off radio button in the Flow Control field of the Physical Configuration table.
5. Click Apply.
6. Click `eth-s2p1c0` in the Logical Interfaces table to go to the *Interface* page.
7. Enter `192.168.4.1` in the New IP Address edit box.
8. Enter `24` in the New Mask Length edit box.
9. Click Apply.
10. Click the Up button to go the *Interface Configuration* page.
11. Click the On radio button for `eth-s2p1c0`.
12. Click Apply.
13. Click Save.

8

Creating VLAN interfaces

Before you start

In order to VLAN interfaces, you need to be on the configuration page of the correct physical Ethernet interface:

1. Click **Config** on the Voyager home page.
2. Click the *Interfaces* link.
3. Click the name of the correct physical Ethernet interface in the **Physical** column.



Steps

1. **Enter a new VLAN ID.**

Enter a value to identify the VLAN interface in the **Create A New VLAN ID** edit box.

The range is 2 to 4094. The values 0 and 4095 are reserved by the IEEE standard. VLAN ID 1 is reserved by convention. There is no default.

2. **Click Apply.**

Expected outcome

The new logical interface for the VLAN appears in the **Logical Interfaces** field. The name of the interface is of the type `eth-sXpYcZ`, where X is the slot number, Y is the physical port number and Z is the channel number. The channel numbers increment starting with 1 with each VLAN ID that you create.

3. *If you want to create more VLAN interfaces*

Then

Repeat the procedure.

Else

Configure the interfaces you have created.

Continue by completing the steps in *Configuring logical Ethernet and VLAN interfaces* for each VLAN interface you have created.

Further information

See *Virtual LAN interfaces* and *Deleting logical interfaces*

9

Deleting logical interfaces



Steps

1. **Go to the configuration page of the correct physical interface.**

In order to remove logical interfaces, you need to be on the configuration page of the appropriate physical interface:

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.
- c. Click the link of the correct physical interface in the **Physical** column.

2. **Select the logical interfaces you want to delete.**

Click the check box in the **Delete** column next to the logical interfaces you want to delete.

3. **Click Apply.**

Expected outcome

The logical interface disappears from the list.

4. **To make your changes permanent, click Save.**

10 Configuring physical ATM interfaces



Steps

1. Go to the Interface Configuration page of the Voyager.

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.

2. Select the physical interface to configure.

Click the physical interface link you want to configure in the **Physical** column. For example, click `atm-s2p1`.

Expected outcome

The configuration page for the selected physical interface opens.

3. Select the framing format.

Select **SONET** or **SDH** as the framing format in the **Physical Configuration** table. The setting should match the type of transmission network to which the interface is connected.

Note

SONET and SDH settings are available only if the ATM interface card supports them.

4. Select the transmit clock.

Select **Freerun** or **Loop Timing** as the transmit clock choice in the **Physical Configuration** table.

Note

The Transmit Clock settings are available only if the ATM interface card supports them.

Further information

Freerun uses the internal clock. If two ATM interfaces are directly connected, at least one of them must use the internal clock.

Loop timing derives the transmit clock from the recovered receive clock.

5. **Click Apply.**
6. *If Logical interfaces need to be created.*

Then

Continue from Creating logical ATM interfaces.

7. **To make your changes permanent, click Save.**

Further information

See *ATM point-to-point interface configuration example* and *IP over ATM configuration example*

11

Creating logical ATM interfaces

Before you start

In order to create logical interfaces, you need to be on the configuration page of the appropriate physical interface:

1. Click **Config** on the Voyager home page.
2. Click the *Interfaces* link.
3. Click the physical interface link you want to configure in the **Physical** column.



Steps

1. **Select the VCI/VPI range.**

Select the VPI/VCI range in the **VPI/VCI Range Configuration** selection box.

2. **Select the type of the logical interface.**

Select **Point-to-Point** or **LIS** (Logical IP Subnet) in the **Type** selection box in the *Create a new LLC/SNAP RFC1483 interface* section.

3. *If the type of the interface is point-to-point*

Then

Enter the VPI/VCI number of the point-to-point interface in the VPI/VCI edit box.

Else

Enter a set of VPI/VCI numbers for the LIS interface.

For LIS, the set of VPI/VCI numbers can be given as a comma-separated list of VPI/VCI numbers, or VPI/VCI ranges such as 1/42, 1/48, 1/50-60. See the following table for ranges:

VPI Range	VCI Range
0	1 - 4095
0 - 1	1 - 2047
0 - 3	1 - 1023
0 - 255	1 - 15

4. Click Apply.

Expected outcome

A new logical interface appears in the **Interface** column. The new interface is turned on by default.

5. If you want to create more interfaces

Then

Repeat this procedure.

Else

Configure the logical interfaces.

To configure the interfaces you have created, complete one of these procedures for each interface:

- *Configuring ATM point-to-point interfaces*
- *Configuring ATM LIS interfaces*

Further information

You can create multiple logical interfaces by repeating this procedure.

For more information, see *Deleting logical interfaces*, *ATM point-to-point interface configuration example* and *IP over ATM configuration example*

12

ATM point-to-point interface configuration example

Purpose

This section describes how you might configure the interfaces of your network application platform (NAP) in an example network, using Voyager.

Before you start

Before you can configure interfaces using Voyager, you must first configure an IP address on one of the interfaces. You can do this through the unit console port during installation or by using the Lynx browser. This allows a graphical browser such as Internet Explorer or Netscape Navigator to access the unit through that interface. You can use any graphical web browser to configure the other interfaces on the NAP by entering the IP address of the NAP in the location field of the browser.

The figure below shows the network configuration for this example.

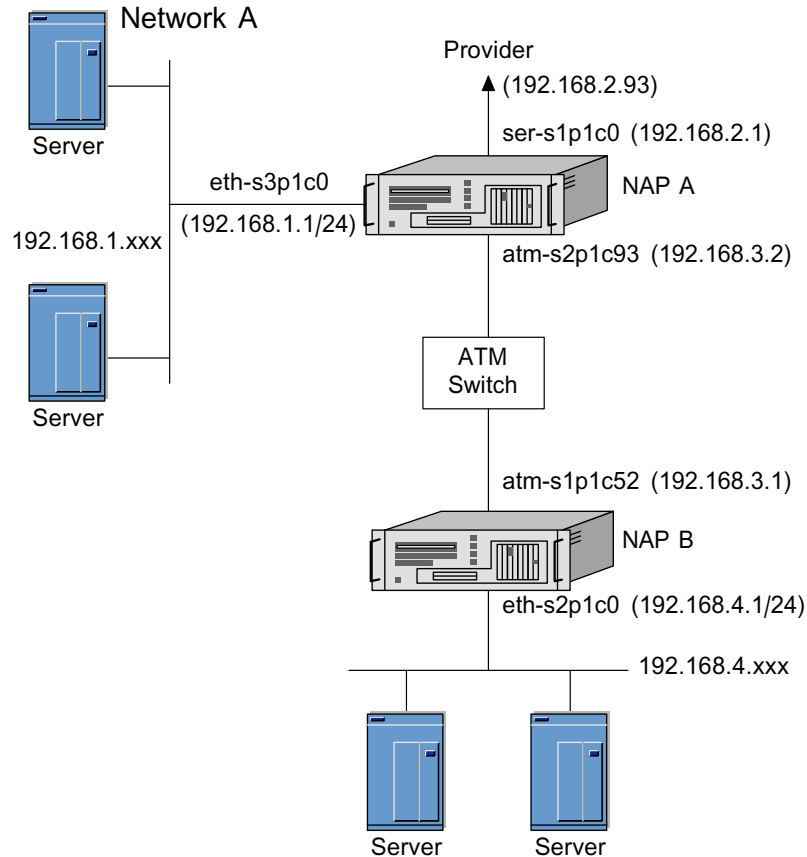


Figure 5. Example of network configuration for an ATM interface

In a company's main office, NAP A terminates a serial line to an Internet service provider, running PPP with a keepalive value of 10. NAP A also provides internet access for Network A and a remote branch office connected via ATM PVC 93.

The branch office contains NAP B, which routes traffic between a local Fast Ethernet network and ATM PVC 52. It provides access to the main office and the Internet. We are configuring the ATM interface on NAP A.



Steps

1. Click **Config** on the home page.
2. Click the **Interfaces** link.
3. Select `atm-s2p1` in the **Physical** column of the table.

4. **Select VPI VCI range Configuration as 0 only/1-4095**
5. **Select Type as "point-to-point" and enter 0/93 in the VPI/VCI edit box in the Create a new LLC/SNAP RFC1483 interface section.**
6. **Click Apply.**
7. **Click atm-s2p1c93 in the Logical Interfaces table to go to the *Interface* page.**

The channel number is automatically generated.

8. **Enter 192.168.3.2 in the Local Address edit box.**
9. **Enter 192.168.3.1 in the Remote Address edit box.**
10. **Click Apply.**
11. **Enter 1500 in the IP MTU edit box.**

The default the value is 1500.

12. **Click Apply.**
13. **Click Save.**

13 IP over ATM configuration example

Purpose

This section describes how you might configure the interfaces of your network application platform (NAP) in an example network, using Voyager.

Before you start

Before you can configure interfaces using Voyager, you must first configure an IP address on one of the interfaces. You can do this through the NAP console port during installation or by using the Lynx browser. This allows a graphical browser such as Internet Explorer or Netscape Navigator to access the NAP through that interface. You can use any graphical web browser to configure the other interfaces on the NAP by entering the IP address of the NAP in the location field of the browser.

The figure below shows the network configuration for this example.

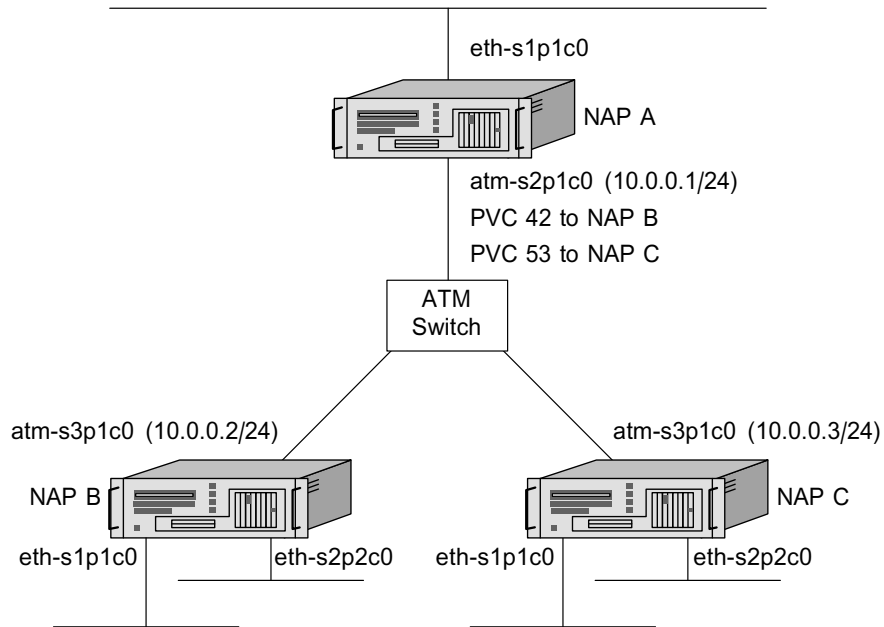


Figure 6. Example of network configuration for IPoA

A company has five ethernet networks in three separate locations. The networks are connected to each other using three routers that belong to the same logical IP subnet over ATM. We are configuring the ATM interface on NAP A. The interface is connected to NAP B via ATM PVC 42 and to NAP C via ATM PNC 53. NAP B and NAP C are connected to each other via an ATM PVC; their ATM interfaces have already been configured.



Steps

1. Click **Config** on the home page.
2. Click the **Interfaces** link.
3. Click the **physical interface link you want to configure in the Physical column.**

For example, atm-s2p1.

Expected outcome

You are taken to the *Physical Interface* page.

4. **Create a logical interface using the *Create a new LLC/SNAP RFC1483 interface* section by selecting LIS in the Type selection box.**
5. **Enter 42 , 53 in the VCI(S) edit box.**
6. **Click Apply.**
7. **Click the newly created interface (atm-s2p1c0) in the Logical Interfaces table to reach the *Logical Interface* page.**
8. **Enter 10.0.0.1 in the IP Address edit box.**
9. **Enter 24 in the Mask Length edit box.**
10. **Click Apply.**
11. **Click Save.**

14 Configuring physical serial interfaces



Steps

1. Go to the Interface Configuration page of the Voyager.

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.

2. Select the physical interface to configure.

Click the physical interface link you want to configure in the **Physical** column. For example, `ser-s2p1`.

3. (Optional) Enable or disable the internal clock. Click Apply.

Click **On** or **Off** in the **Internal Clock** field to enable or disable the internal clock on the serial device. Click **Apply**.

If you're connecting to a device or system that does not provide a clock source, enable the internal clock. Otherwise, disable the internal clock.

4. If you enabled the internal clock

Then

Enter the speed for the internal clock.

Enter a value in the **Internal Clock Speed** edit box to define the speed of the internal clock.

Further information

If the device can generate only certain line rates, and the configured line rate is not one of these values, the device selects the next highest available line rate.

5. Select the channel mode.

Click the **Full Duplex** or **Loopback** radio button in the **Channel Mode** field. Full duplex is the normal mode of operation.

6. Select the encapsulation.

Select the encapsulation in the **Encapsulation** field. For serial interfaces, the encapsulation can be **Cisco HDLC**, **PPP** or **Frame Relay**.

7. Click Apply.

Expected outcome

If you selected **Cisco HDLC** or **PPP** as the encapsulation, a logical interface appears in the **Logical Interfaces** table.

8. Configure the encapsulation protocol.

To configure the encapsulation protocol you selected, complete one of these procedures:

- *Configuring Cisco HDLC protocol*
- *Configuring PPP protocol*
- *Configuring Frame Relay protocol*

Further information

See *Serial interface configuration example*

15

Configuring ATM point-to-point interfaces



Steps

1. **Go to the configuration page of the logical interface.**

In order to configure a logical interface, you need to be on the configuration page of the logical interface:

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.
- c. Click the logical interface link you want to configure in the **Logical** column.

Click the name of the logical interface on the configuration page of the appropriate physical interface.

2. *If you want to change the existing local and remote IP addresses*

Then

Delete the current IP addresses.

Before you start

Note

Do not change the IP address you use in your browser to access Voyager. If you do, you can no longer access the network application platform (NAP) with your browser.

-
- a. Delete the address from the **Local Address** edit box.
 - b. Delete the address from the **Remote Address** edit box.
 - c. Click **Apply**.

Expected outcome

This removes the old IP address pair. The MTU value is not changed.

3. Enter the IP address for the local end.

Enter the IP address for the local end of the link in the **Local Address** edit box.

4. Enter the IP address for the remote end.

Enter the IP address for the remote end of the link in the **Remote Address** edit box.

5. Enter the MTU length (in bytes).

Enter a number in the IP MTU edit box to configure the maximum length (in bytes) of IP packets transmitted in this interface. The default value is 1500 for the PTP interface (IP740 maximum is 9180, IP3400 maximum is 2008, only for LIS interfaces).

If you do not want to change the current MTU value, you can skip this step.

Note

The MTU length must match the MTU length of the link partner. Packets longer than the MTU length will be fragmented before transmission.

6. (Optional) Change the logical name of the interface.

Change the interface's logical name to a more meaningful one by typing the preferred name in the **Logical Name** edit box.

7. Click Apply.**Expected outcome**

This adds a new IP address pair. If you entered a new MTU value, the new value replaces the old value.

8. To make your changes permanent, click Save.

Further information

See *Creating logical ATM interfaces*, *Deleting logical interfaces* and *ATM point-to-point interface configuration example*

16

Configuring ATM LIS interfaces



Steps

1. **Go to the configuration page of the correct physical interface.**

In order to configure an ATM LIS interface, you need to be on the configuration page of the appropriate physical interface:

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.
- c. Click the physical interface link you want to configure in the **Physical** column.

2. *If the current VPI/VCIs need to be changed*

Then

Delete the existing VPI/VCIs of the interface, and create a new one by following the steps below.

Before you start

Note

Do not change the VCI address of the connection you are using. If you do, you can no longer access the network application platform (NAP) with your browser.

- a. Select the VPI/VCI range in the **VPI/VCI Range Configuration** selection box.
- b. Select type as LIS in **Create new LLC/SNAP interface**.
- c. Enter a new set of VPI/VCIs in the **VPI/VCI** field of the interface.
- d. Click **Apply**.

3. **Go to the logical interface configuration page.**

Click the name of the logical interface on the configuration page of the appropriate physical interface.

4. Enter the IP address.

Enter the IP address for the interface in the **IP Address** edit box.

5. Enter the subnet mask length.

Enter the subnet mask length in the **Mask Length** edit box.

6. Enter the MTU length (in bytes).

Enter a number in the IP MTU edit box to configure the maximum length (in bytes) of IP packets transmitted in this interface. The default values are 9180 (IP740) and 2008 (IP3400)

If you do not want to change the current MTU value, you can skip this step.

Note

All hosts in the same LIS must use the same MTU length in their interface to the LIS. Packets longer than the MTU length will be fragmented before transmission.

7. (Optional) Change the logical name of the interface.

Change the interface's logical name to a more meaningful one by typing the preferred name in the **Logical Name** edit box.

8. Click Apply.

9. To make your changes permanent, click Save.

Further information

See *Creating logical ATM interfaces* and *Deleting logical interfaces*

17 Serial interface configuration example

Purpose

This section describes how you might configure the interfaces of your network application platform (NAP) in an example network, using Voyager.

Before you start

Before you can configure the unit using Voyager, you must first configure an IP address on one of the interfaces. You can do this through the unit console port during installation or by using the Lynx browser. This allows a graphical browser such as Internet Explorer or Netscape Navigator to access the unit through that interface. You can use any graphical web browser to configure the other interfaces on the NAP by entering the IP address of the NAP in the location field of the browser.

The figure below shows the network configuration for this example.

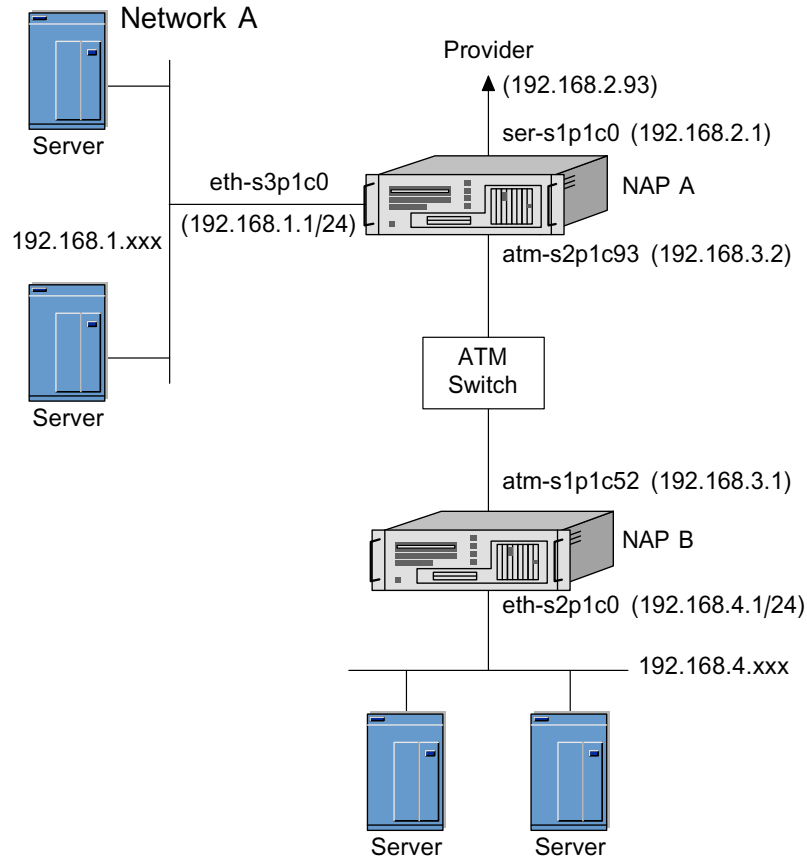


Figure 7. Example of network configuration for serial interfaces

In a company's main office, NAP A terminates a serial line to an Internet service provider, running PPP with a keepalive value of 10. NAP A also provides internet access for Network A and a remote branch office connected via ATM PVC 93.

The branch office contains NAP B, which routes traffic between a local Fast Ethernet network and ATM PVC 52. It provides access to the main office and the Internet. We are configuring the serial interface on NAP A.



Steps

1. Click **Config** on the home page.
2. Click the **Interfaces** link.
3. Select **ser-s1p1** in the **Physical** column of the table.

4. Click the PPP radio button in the Encapsulation field.
5. Click Apply.
6. Enter 10 in the Keepalive edit box.
7. Click Apply.
8. Click `ser-s1p1c0` in the Logical Interfaces table to go to the *Interface* page.
9. Enter 192.168.2.1 in the Local Address edit box.
10. Enter 192.168.2.93 in the Remote Address edit box.
11. Click Apply.
12. Click the Up button to go to the *Interfaces* page.
13. Click the On radio button for `ser-s1p1c0`.
14. Click Apply.
15. Click Save.

18 Configuring Cisco HDLC protocol



Steps

1. **Go to the Interface Configuration page of the physical interface.**
 - a. Click **Config** on the Voyager home page.
 - b. Click the *Interfaces* link.
 - c. Click the physical interface link you want to configure in the **Physical** column.

2. **Enter the keepalive interval.**

Enter a number in the **Keepalive** edit box of the **Physical Configuration** table to configure the Cisco HDLC keepalive interval.

Further information

This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

Note

This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

3. **Click Apply.**
4. **Go to the configuration page of the logical interface.**

Click the logical interface name in the **Interface** column of the **Logical Interfaces** table to go to the *Interface* page.

5. *If you want to change the existing local and remote IP addresses*

Then

Delete the current IP addresses.

Before you start

Note

Do not change the IP address you use in your browser to access Voyager. If you do, you can no longer access the network application platform (NAP) with your browser.

- a. Delete the address from the **Local Address** edit box.
- b. Delete the address from the **Remote Address** edit box.
- c. Click **Apply**.

Expected outcome

This removes the old IP address pair.

6. Enter the IP address for the local end.

Enter the IP address for the local end of the link in the **Local Address** edit box.

7. Enter the IP address for the remote end.

Enter the IP address for the remote end of the link in the **Remote Address** edit box.

8. (Optional) Change the logical name of the interface.

Change the interface's logical name to a more meaningful one by typing the preferred name in the **Logical Name** edit box.

9. Click Apply.

Expected outcome

This adds a new IP address pair.

10. To make your changes permanent, click Save.

Further information

See *Deleting logical interfaces*, *Serial interface configuration example* and *T1 interface configuration example*

19

Configuring physical T1 interfaces



Steps

1. Go to the Interface Configuration page of the Voyager.

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.

2. Select the physical interface to configure.

Click the physical interface link you want to configure in the **Physical** column. For example, `ser-s2p1`.

3. (Optional) Enable or disable the internal clock.

Click **On** or **Off** in the **Internal Clock** field to enable or disable the internal clock on the T1 device. Click **Apply**.

If you're connecting to a device or system that does not provide a clock source, enable the internal clock. Otherwise, disable the internal clock.

Further information

Internal clocking for T1 is fixed at 1.544 Mbits/s. To configure slower speeds, you must configure fractional T1 on the *Advanced T1 CSU/DSU Options* page.

4. Select the channel mode.

Click the **Full Duplex** or **Loopback** radio button in the **Channel Mode** field. Full duplex is the normal mode of operation.

5. Select the T1 encoding.

Click the **AMI** or **HDB3** radio button in the **T1 Encoding** field to select the T1 encoding. Click **Apply**.

This setting must match the line encoding of the CSU/DSU at the other end of the point-to-point link.

6. Select T1 framing format.

Click the **Superframe (D4)** or the **Extended SF** radio button in the **T1 Framing** field to select the T1 Framing format. Click **Apply**.

This setting must match the frame format used by the CSU/DSU at the other end of the point-to-point link.

Further information

Use T1 framing to divide the data stream into 64Kbps channels and to synchronize with the remote CSU/DSU.

7. Select the speed of the DS0 channel.

Click the **64Bps** or **56Bps** radio button in the **T1 Channel Speed** field to select the DS0 channel speed for the T1 line.

Further information

Some older trunk lines use the least-significant bit of each DS0 channel in a T1 frame for switching-equipment signalling. T1 frames designed for data transfer can be set to not use the least-significant bit of each DS0 channel. This setting allows data to be sent over these trunk lines without corruption but at a reduced throughput. This mode is called the 56Kbps mode because each DS0 channel now has an effective throughput of 56Kbps instead of 64Kbps. All T1 functions still work in the 56Kbps mode, including all framing modes and fractional T1 configurations.

8. If you selected **Extended SF as the framing format**

Then

Select the FDL type.

Click **ANSI** or **NONE** in the **FDL Type** field to select the FDL type.

9. Select the encapsulation.

Select the encapsulation in the **Encapsulation** field. For T1 interfaces, the encapsulation can be **Cisco HDLC**, **PPP** or **Frame Relay**.

10. Click Apply.

Expected outcome

If you selected **Cisco HDLC** or **PPP** as the encapsulation, a logical interface appears in the **Logical Interfaces** table.

11. (Optional) Configure Advanced T1 CSU/DSU Options.

Click the *Advanced T1 CSU/DSU Options* link to select advanced E1 options.

To return to the physical interface page from the *Advanced T1 CSU/DSU Options* page, click the **Up** button.

Further information

The *T1 CSU/DSU Advanced Options* page allows you to configure fractional T1 channels, line build-out values and other advanced settings for the T1 device.

Note

The values you enter on this page are dependent on the subscription provided by your service provider.

12. Configure the encapsulation protocol.

To configure the encapsulation protocol you selected, complete one of these procedures:

- *Configuring Cisco HDLC protocol*
- *Configuring PPP protocol*
- *Configuring Frame Relay protocol*

Further information

See *T1 interface configuration example*

20 T1 interface configuration example

Purpose

This section describes how you might use Voyager to configure the interfaces of your network application platform (NAP) in an example network.

Before you start

Before you can configure the unit using Voyager, you must first configure an IP address on one of the interfaces. You can do this through the console port during installation or by using the Lynx browser. This procedure allows a graphical browser such as Internet Explorer or Netscape Navigator to access the unit through that interface. You can use any graphical web browser to configure the other interfaces on the NAP by entering the IP address of the NAP in the location field of the browser.

The figure below shows the network configuration for this example.

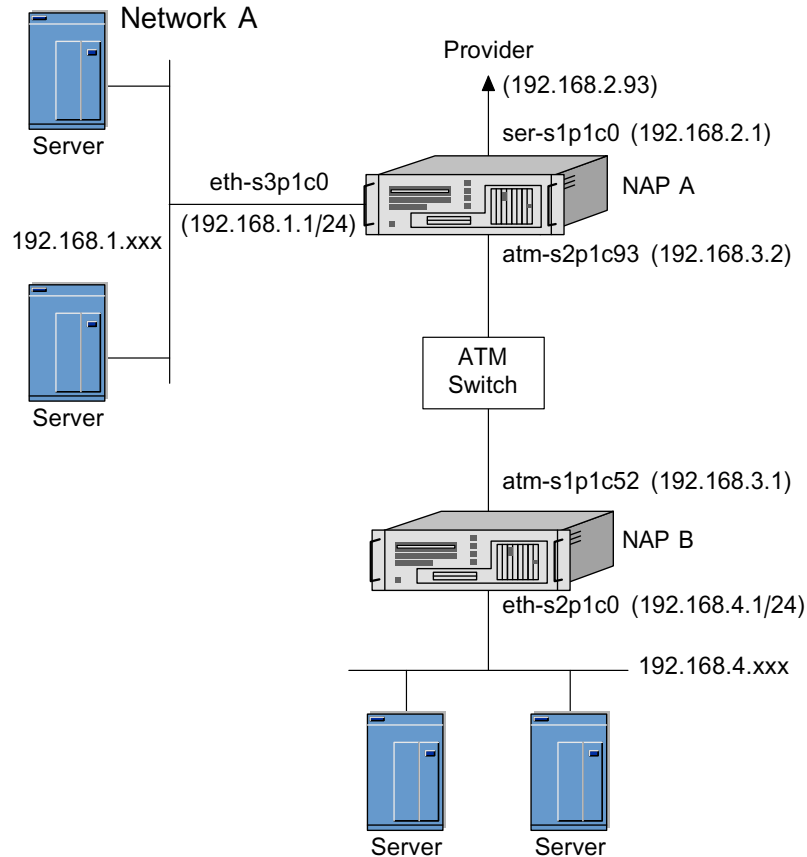


Figure 8. Example of network configuration for T1

In a company's main office, NAP A terminates a T1 line to an Internet service provider, running PPP with a keepalive value of 10. The T1 line uses B8ZS line encoding, Extended Super Frame, T1 framing, and 64 Kbps channels.

NAP A also provides internet access for Network A and a remote branch office connected via ATM PVC 93.

The branch office contains NAP B, which routes traffic between a local Fast Ethernet network and ATM PVC 52. It provides access to the main office and the Internet. We are configuring the serial interface on NAP A.



Steps

1. Click **Config** on the home page.
2. Click the **Interfaces** link.

3. Select `ser-s1p1` in the Physical column of the table.
4. Click the B8ZS radio button in the T1 Encoding field.
5. Click the Extended SF radio button in the T1 Framing field.
6. Click the 64 Kbps radio button in the T1 Channel Speed field.
7. Click the PPP radio button in the Encapsulation field.
8. Click Apply.
9. Enter 10 in the Keepalive edit box.
10. Click Apply.
11. Click `ser-s1p1c0` in the Logical Interfaces table to go to the *Interface* page.
12. Enter 192.168.2.1 in the Local Address edit box.
13. Enter 192.168.2.93 in the Remote Address edit box.
14. Click Apply.
15. Click the Up button to go to the *Interfaces* page.
16. Click the On radio button for `ser-s1p1c0`.
17. Click Apply.
18. Click Save.

21

Configuring physical E1 interfaces



Steps

1. Go to the Interface Configuration page of the Voyager.

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.

2. Select the physical interface to configure.

Click the physical interface link you want to configure in the **Physical** column. For example, `ser-s2p1`.

3. (Optional) Enable or disable the internal clock.

Click **On** or **Off** in the **Internal Clock** field to enable or disable the internal clock on the E1 device. Click **Apply**.

If you're connecting to a device or system that does not provide a clock source, enable the internal clock. Otherwise, disable the internal clock.

Further information

Internal clocking for E1 is fixed at 2.048 Mbits/sec. To configure slower speeds, you must configure fractional E1 on the *Advanced E1 CSU/DSU Options* page.

4. Select the channel mode.

Click the **Full Duplex** or **Loopback** radio button in the **Channel Mode** field. Full duplex is the normal mode of operation.

5. Select the E1 encoding.

Click the **AMI** or **HDB3** radio button in the **E1 Encoding** field to select the E1 encoding. Click **Apply**.

This setting must match the line encoding of the CSU/DSU at the other end of the point-to-point link.

6. Select E1 framing format.

Click the **E1** (channel 0 framing) or the **No Framing** radio button in the **E1 Framing** field to select the E1 framing format. Click **Apply**.

Further information

Use E1 framing to select whether timeslot-0 is used for exchanging signaling data.

7. If you selected E1 (channel 0 framing) as the framing format

Then

Enable or disable CRC-4 framing.

Click the **On** or **Off** radio button for the **E1 CRC-4 Framing** field.

This setting must match the setting of the CSU/DSU at the other end of the link.

Further information

This button chooses the framing format for timeslot-0. **On** means that CRC-multiframe format is used; the information is protected by CRC-4. **Off** means that double-frame format is used.

Note

This option appears only if you have set the **E1 Framing** field to E1 (CHANNEL 0 FRAMING).

8. If you selected E1 (channel 0 framing) as the framing format

Then

Enable or disable E1 timeslot-16 framing.

Click the **On** or **Off** radio button for the E1 TIMESLOT-16 FRAMING. Click **Apply**.

Further information

This value controls whether timeslot-16 is used in channel associated signaling (CAS). Setting this value to **On** means that timeslot-16 cannot be used as a data channel.

For more information, see fractional settings on the *Advanced E1 CSU/DSU Options* page.

Note

This option appears only if you have set the **E1 Framing** field to E1 (CHANNEL 0 FRAMING).

9. Select the encapsulation.

Select the encapsulation in the **Encapsulation** field. For E1 interfaces, the encapsulation can be **Cisco HDLC**, **PPP** or **Frame Relay**.

10. Click Apply.

Expected outcome

If you selected **Cisco HDLC** or **PPP** as the encapsulation, a logical interface appears in the **Logical Interfaces** table.

11. (Optional) Configure Advanced E1 CSU/DSU Options.

Click the *Advanced E1 CSU/DSU Options* link to select advanced E1 options.

To return to the physical interface page from the *Advanced E1 CSU/DSU Options* page, click the **Up** button.

Further information

The *E1 CSU/DSU Advanced Options* page allows you to configure fractional E1 channels and other advanced settings for the E1 device.

Note

The values you enter on this page are dependent on the subscription provided by your service provider.

12. Configure the encapsulation protocol.

To configure the encapsulation protocol you selected, complete one of these procedures:

- *Configuring Cisco HDLC protocol*
- *Configuring PPP protocol*
- *Configuring Frame Relay protocol*

22 Managing unnumbered interfaces

Purpose

Note

Only point-to-point interfaces can be configured as unnumbered interfaces. Tunnels cannot be configured as unnumbered interfaces.

Note

You must choose a proxy interface for the unnumbered interface to function.



Steps

1. **Go to the configuration page of the correct logical interface.**

In order to configure a logical interface, you need to be on the configuration page of that logical interface:

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.
- c. Click the logical interface link you want to configure in the **Logical** column.

For example, atm s3p1c1.

2. *If you are configuring a numbered interface to unnumbered*

Then

Click the Yes radio button in the Unnumbered Interface field and click Apply.

Further information

Note

If that interface was associated with either a local or remote address or both, they are automatically deleted.

Note

You do not see local and remote address configuration fields for unnumbered interfaces. The proxy interface field replaces those fields.

Note

The interface must not be used by a tunnel, and OSPF is the only protocol that the interface can be running.

Else

If you are configuring an unnumbered interface to numbered

Then

Click the No radio button in the Unnumbered Interface field.

Further information

Note

This interface must not be the next hop of a static route.

Note

After completing the procedure, you must configure a numbered logical interface.

3. *If you selected Yes in the previous step*

Then

Select an interface from the Proxy Interface drop-down window.

Further information

Note

The **Proxy Interface** drop-down window shows only those interfaces that have been assigned addresses.

Note

You cannot delete the only IP address of the proxy interface. First, select another proxy interface and then delete the IP address of the original proxy interface. If the proxy interface has multiple IP addresses associated with it, you can delete or add addresses. A proxy interface must have at least one IP address associated with it.

4. Click Apply.

5. To make your changes permanent, click Save.

Further information

See *Unnumbered interfaces* and *Configuring a static route over an unnumbered interface*

23

Configuring a static route over an unnumbered interface

Purpose

Note

You select an unnumbered logical interface as the next-hop gateway when you do not know the IP address of the next-hop gateway.

Before you start

The interface must be configured as unnumbered. For instructions, see *Managing unnumbered interfaces*.



Steps

1. Go to the Static Routes page.

In order to configure a static route, you need to be on the Static Routes page:

- a. Click **Config** on the Voyager home page.
- b. Click the *Static Routes* link under the *Routing Configuration* section.

2. Enter the IP address of the destination network.

Enter the IP address of the destination network in the **New Static Route** edit box.

3. Enter the mask length (in bits).

mask length (in bits) in the **Mask Length** edit box.

4. Select the type of next hop for the static route.

Select the type of next hop the static route will take from the **Next Hop Type** drop-down window. Your options are **Normal**, **Reject**, and **Black Hole**. The default is **Normal**.

5. Select Gateway Logical as the next-hop gateway type.

Select **Gateway Logical** as the next-hop gateway type from the **Gateway Type** drop-down window.

6. Click Apply.

7. Select the next-hop gateway.

Click on the **Gateway Logical** drop-down window to view the list of unnumbered interfaces that are configured. Select the unnumbered logical interface you want to use as a next-hop gateway to the destination network.

8. Click Apply.

9. To make your changes permanent, click Save.

Further information

See *Unnumbered interfaces*

24

Configuring OSPF over an unnumbered interface

Summary

The graphic below represents an example configuration for running OSPF over an unnumbered interface.

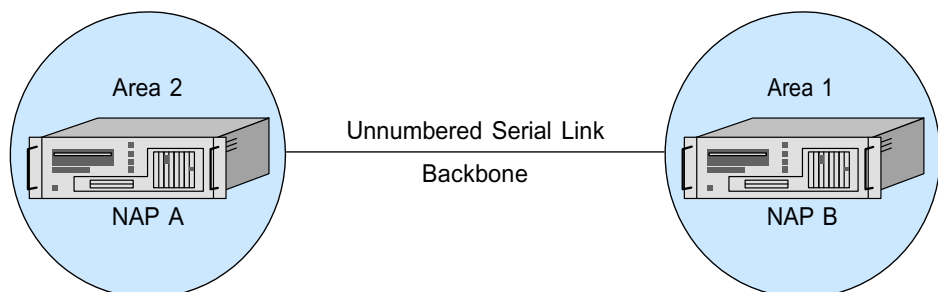


Figure 9. Example configuration for running OSPF over an unnumbered interface



Steps

1. Configure NAP A and NAP B as unnumbered.

Configure the interfaces on NAP A and NAP B as unnumbered. For instructions, see *Managing unnumbered interfaces*.

2. Configure OSPF areas.

For each NAP, configure an OSPF area as in *Configuring OSPF / OSPFv3*.

3. Select backbone as the area for the unnumbered interfaces.

In the **Interfaces** section, click on the **Area** drop-down window next to the configured unnumbered interfaces and select **Backbone**.

Further information

Note

Because the unnumbered interface uses the selected proxy interface's IP address, whenever you change this proxy interface, OSPF adjacencies are re-established.

Note

Whenever you change the unnumbered serial interface's underlying encapsulation, for example from Cisco HDLC to PPP or from PPP to Frame Relay, OSPF adjacencies are re-established.

25 Configuring PPP protocol



Steps

1. **Go to the Interface Configuration page of the physical interface.**
 - a. Click **Config** on the Voyager home page.
 - b. Click the *Interfaces* link.
 - c. Click the logical interface link you want to configure in the **Logical** column.

2. **Enter the keepalive interval.**

Enter a number in the **Keepalive** edit box of the **Physical Configuration** table to configure the PPP keepalive interval.

Further information

This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

Note

This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

3. **Enter a maximum number of failures for the keepalive message.**

Enter a number in the **Keepalive Maximum Failures** edit box.

Further information

This value sets the number of times a remote system may fail to send a keepalive protocol message within a keepalive interval before the systems considers the link down.

4. Click the **Advanced PPP Options** link.

Expected outcome

The *PPP Advanced Options* page appears.

5. **Enable or disable magic number negotiation.**

Click **Yes** or **No** in the **Negotiate Magic Number** field. Clicking **Yes** enables the interface to send a request to negotiate a magic number with a peer.

6. **Enable or disable MRU negotiation.**

Click **Yes** or **No** in the **Negotiate Maximum Receive Unit** field. Clicking **Yes** enables the interface to send a request to negotiate an MRU with a peer.

7. Click **Apply**.

8. Click **Up**.

Click **Up** to return to the **Physical Interface** page.

9. **Go to the configuration page of the logical interface.**

Click the logical interface name in the **Interface** column of the **Logical Interfaces** table to go to the *Interface* page.

10. *If you want to change the existing local and remote IP addresses*

Then

Delete the current IP addresses.

Before you start

Note

Do not change the IP address you use in your browser to access Voyager. If you do, you can no longer access the network application platform (NAP) with your browser.

- a. Delete the address from the **Local Address** edit box.
- b. Delete the address from the **Remote Address** edit box.
- c. Click **Apply**.

Expected outcome

This removes the old IP address pair.

11. Enter the IP address for the local end.

Enter the IP address for the local end of the link in the **Local Address** edit box.

12. Enter the IP address for the remote end.

Enter the IP address for the remote end of the link in the **Remote Address** edit box.

13. (Optional) Change the logical name of the interface.

Change the interface's logical name to a more meaningful one by typing the preferred name in the **Logical Name** edit box.

14. Click Apply.**Expected outcome**

This adds a new IP address pair.

15. To make your changes permanent, click Save.**Further information**

See *Deleting logical interfaces*, *Serial interface configuration example* and *T1 interface configuration example*

26 Configuring frame relay protocol



Steps

1. **Go to the Interface Configuration page of the physical interface.**
 - a. Click **Config** on the Voyager home page.
 - b. Click the *Interfaces* link.
 - c. Click the logical interface link you want to configure in the **Logical** column.

2. **Enter the keepalive interval.**

Enter a number in the **Keepalive** edit box of the **Physical Configuration** table to configure the frame relay keepalive interval.

Further information

This value sets the interval, in seconds, between keepalive protocol message transmissions. These messages are used periodically to test for an active remote system.

Note

This value must be identical to the keepalive value configured on the system at the other end of a point-to-point link, or the link state fluctuates.

3. **Select the interface type.**

Click the **DTE** or **DCE** radio button in the **Interface Type** field.

DTE is the usual operating mode when the device is connected to a frame relay switch.

4. **Enable or disable the monitoring of connection-active status.**

Click the **On** or **Off** radio button in the **Active Status Monitor** field. This sets the monitoring of the connection-active status in the LMI status message.

5. (Optional) Configure frame relay advanced options.

Click the *Advanced Frame Relay Options* link to go to the *Frame Relay Advanced Options* page. To return to the physical interface page from the *Frame Relay Advanced Options* page, click the **Up** button.

Further information

The *Frame Relay Advanced Options* page allows you to configure frame relay protocol and LMI parameters for this device.

Note

The values you enter are dependent on the settings of the frame relay switch to which you are connected or to the subscription provided by your service provider.

6. Configure frame relay PVC.

- a. Enter the DLCI number for the new PVC in the **Create a New Interface DLCI** edit box.
- b. Click **Apply**.

Expected outcome

A new logical interface appears in the **Interface** column. The DLCI number appears as the channel number in the logical interface name. The new interface is turned on by default.

Further information

You can repeat this step to create more PVCs. Remember to repeat all steps after this for each interface you create.

7. Go to the configuration page of the logical interface.

Click the logical interface name in the **Interface** column of the **Logical Interfaces** table to go to the *Interface* page.

8. *If you want to change the existing local and remote IP addresses*
Then

Delete the current IP addresses.**Before you start**

Note

Do not change the IP address you use in your browser to access Voyager. If you do, you can no longer access the network application platform (NAP) with your browser.

- a. Delete the address from the **Local Address** edit box.
- b. Delete the address from the **Remote Address** edit box.
- c. Click **Apply**.

Expected outcome

This removes the old IP address pair.

9. Enter the IP address for the local end.

Enter the IP address for the local end of the link in the **Local Address** edit box.

10. Enter the IP address for the remote end.

Enter the IP address for the remote end of the link in the **Remote Address** edit box.

11. (Optional) Change the logical name of the interface.

Change the interface's logical name to a more meaningful one by typing the preferred name in the **Logical Name** edit box.

12. Click Apply.**Expected outcome**

This adds a new IP address pair.

13. To make your changes permanent, click Save.**14. If you created more than one logical interface**

Then

Configure the other PVCs.

Click the **Up** button to return to the physical interface page. Configure the other PVCs by repeating this procedure from *Step 6*.

Further information

See *Deleting logical interfaces*, *Serial interface configuration example* and *T1 interface configuration example*

27

Configuring loopback interfaces

Purpose

You might want to assign an address to the loopback interface that is the same as the OSPF router ID, or is the termination point of a BGP session. This allows router adjacencies to stay up even if the outbound interface is down.

To change an IP address, first delete the old IP address and then create the new IP address.

Note

The loopback interface always has a logical interface created and enabled.

Before you start

In order to create, change or remove loopback IP addresses, you need to be on the configuration page of the loopback interface:

1. Click **Config** on the Voyager home page.
2. Click the *Interfaces* link.
3. Click the loopback logical interface link in the **Logical** column (loop0c0).



Steps

1. *If you want to remove IP addresses*

Then

Select the IP addresses you want to delete.

Click the check box in the **Delete** column next to the IP addresses you want to delete.

2. *If you want to add an IP address*

Then

Enter the new IP address.

To add an IP address, enter the IP address for the device in the **New IP Address** edit box.

3. **Click Apply.**

Expected outcome

If you selected IP addresses to be deleted, the IP addresses disappear from the table.

If you entered a new IP address, each time you click **Apply** the configured IP address appears in the table. The entry fields remain blank to allow you to add more IP addresses.

4. **To make your changes permanent, click Save.**

Further information

To add or remove more loopback IP addresses, repeat the procedure.

For more information, see *The loopback interface*

28

Creating tunnels



Steps

1. Go to the configuration page of the Tunnels interface.

In order to create tunnels, you need to be on the configuration page of the Tunnels interface:

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.
- c. Click the *Tunnels* link in the **Physical** column.

2. Select the encapsulation type.

Click the drop-down window in the **Create a New Tunnel Interface with Encapsulation** field and select the encapsulation type for the new tunnel (GRE or DVMRP). Click **Apply**.

You can repeat this step to create more tunnels.

Expected outcome

A new tunnel appears in the logical interfaces table.

Further information

GRE tunnels encapsulate IP packets using generic routing encapsulation (GRE) with no options. The encapsulated packets appear as unicast IP packets. GRE tunnels provide redundant configuration between two sites for high availability.

DVMRP tunnels encapsulate multicast packets as IP unicast packets. This feature allows two multicast routers to exchange multicast packets even when they are separated by routers that cannot forward multicast packets.

3. Configure the new tunnel(s).

To configure a tunnel, see *Configuring tunnels*.

Further information

See *Tunnel interfaces*, *Deleting logical interfaces*, *GRE tunnel configuration example*, *HA GRE tunnel configuration example* and *DVMRP tunnel configuration example*

29

Configuring tunnels



Steps

1. Go to the Interface Configuration page of the Voyager.

- a. Click **Config** on the Voyager home page.
- b. Click the *Interfaces* link.

2. Select the tunnel you want to configure.

In the **Logical** column, click the logical interface link of the tunnel you want to configure.

Expected outcome

The *Interface* page for the tunnel opens.

Further information

You can also get to the *Interface* page directly from the configuration page of the Tunnels interface by clicking the tunnel name in the **Interface** column of the Logical interfaces table.

3. Enter the address of the tunnel's local end.

Enter the IP address of the local end of the tunnel in the **Local Address** edit box.

The local address must be the remote address configured on the corresponding tunnel at the remote router.

For GRE tunnels, the local address cannot be one of the system's interface addresses. For DVMRP tunnels, the local address must be one of the system's interface addresses.

4. Enter the address of the tunnel's remote end.

Enter the IP address of the remote end of the tunnel in the **Remote Address** edit box.

The remote address cannot be one of the system's interface addresses.

For GRE tunnels, the remote address must be the local address configured on the GRE tunnel at the remote router.

For DVMRP tunnels, the remote address must be the IP address of the multicast router at the remote end of the DVMRP tunnel.

5. *If you are configuring a GRE tunnel*

Then

Enter the address of the tunnel's local endpoint.

Enter the IP address of the local interface the GRE tunnel is bound to in the **Local Endpoint** edit box.

The local endpoint must be one of the system's interface addresses and must be the remote endpoint configured for the GRE tunnel at the remote router.

6. *If you are configuring a GRE tunnel*

Then

Enter the address of the tunnel's remote endpoint.

Enter the IP address of the remote interface the GRE tunnel is bound to in the **Remote Endpoint** edit box.

The remote endpoint must not be one of the system's interface addresses and must be the local endpoint configured for the GRE tunnel at the remote router.

7. **(Optional) Change the name of the interface.**

Change the interface's logical name to a more meaningful one by typing the preferred name in the **Logical Name** edit box.

8. **Click Apply.**

9. **To make your changes permanent, click Save.**

Further information

See *Tunnel interfaces, Creating tunnels, Deleting logical interfaces, GRE tunnel configuration example, HA GRE tunnel configuration example* and *DVMRP tunnel configuration example*

30 GRE tunnel configuration example

Purpose

The following steps provide directions on how to configure a sample GRE tunnel. The figure below shows the network configuration for this example.

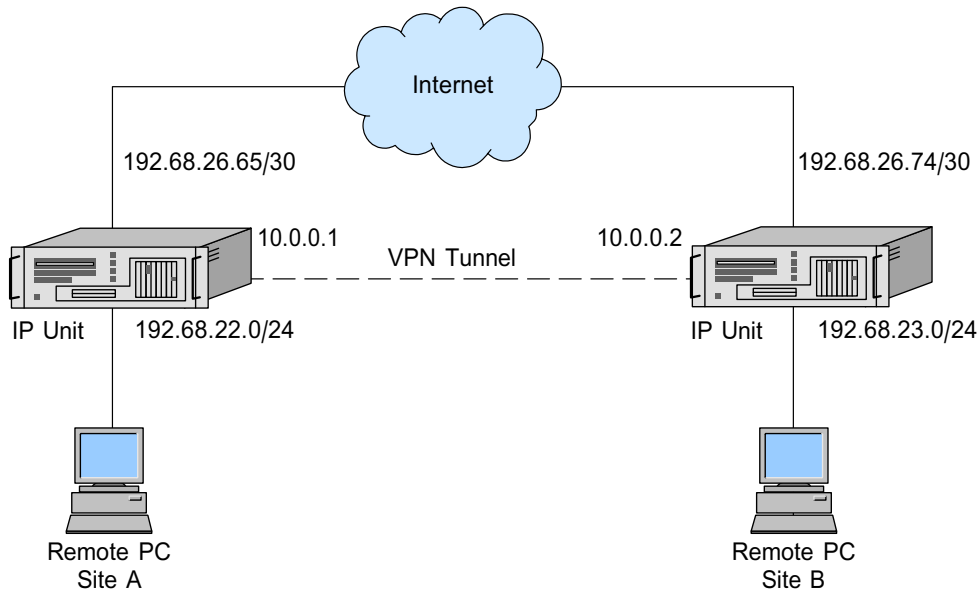


Figure 10. Example of network configuration for GRE tunnel



Steps

1. Click **Config** on the home page.
2. Click the **Interfaces** link.
3. Click **Tunnels** in the **Physical** column.
4. Click the drop-down window in the **Create a New Tunnel Interface** with **Encapsulation** field and select **GRE**.

5. **Click Apply.**
6. **From the Interface column on the Logical Interfaces table, select tun01.**
7. **Enter 10.0.0.1 in the Local Address edit box.**
8. **Enter 10.0.0.2 in the Remote Address edit box.**
9. **Enter 192.68.26.65 in the Local Endpoint edit box.**
10. **Enter 192.68.26.74 in the Remote Endpoint edit box.**
11. **(Optional) Select a value from the TOS Value drop-down window. Click Apply.**

On GRE tunnels, it is desirable to copy or specify the TOS bits when the router encapsulates the packet. After you select the TOS feature, intermediate routers between the tunnel endpoints may take advantage of the QoS features and possibly improve the routing of important packets. By default, the TOS bits are copied from the inner IP header to the encapsulating IP header. If the desired TOS value is not displayed in the drop-down window, select **Custom Value** from the menu. Click **Apply**. An entry field appears.

12. **(Optional) If you selected custom value from the TOS Value drop-down window, enter a value in the range of 0-255. Click Apply.**
13. **(Optional) Change the interface's logical name to a more meaningful one by typing the preferred name in the Logical Name edit box.**
14. **Click Apply.**
15. **To make changes permanent, click Save.**

31 HA GRE tunnel configuration example

Before you start

High availability GRE (HA GRE) tunnels provide redundant encrypted communication among multiple hosts. They are created by performing the procedures associated with the configuration of GRE tunnels, OSPF, and VRRP.

In our example, we configure two-way tunnels between IP Units 1 and 2, and IP Units 3 and 4. Since the steps required to configure a HA GRE tunnel are addressed in the appropriate sections of this reference guide, they will not be individually repeated here. The figure below shows the network configuration for this example.

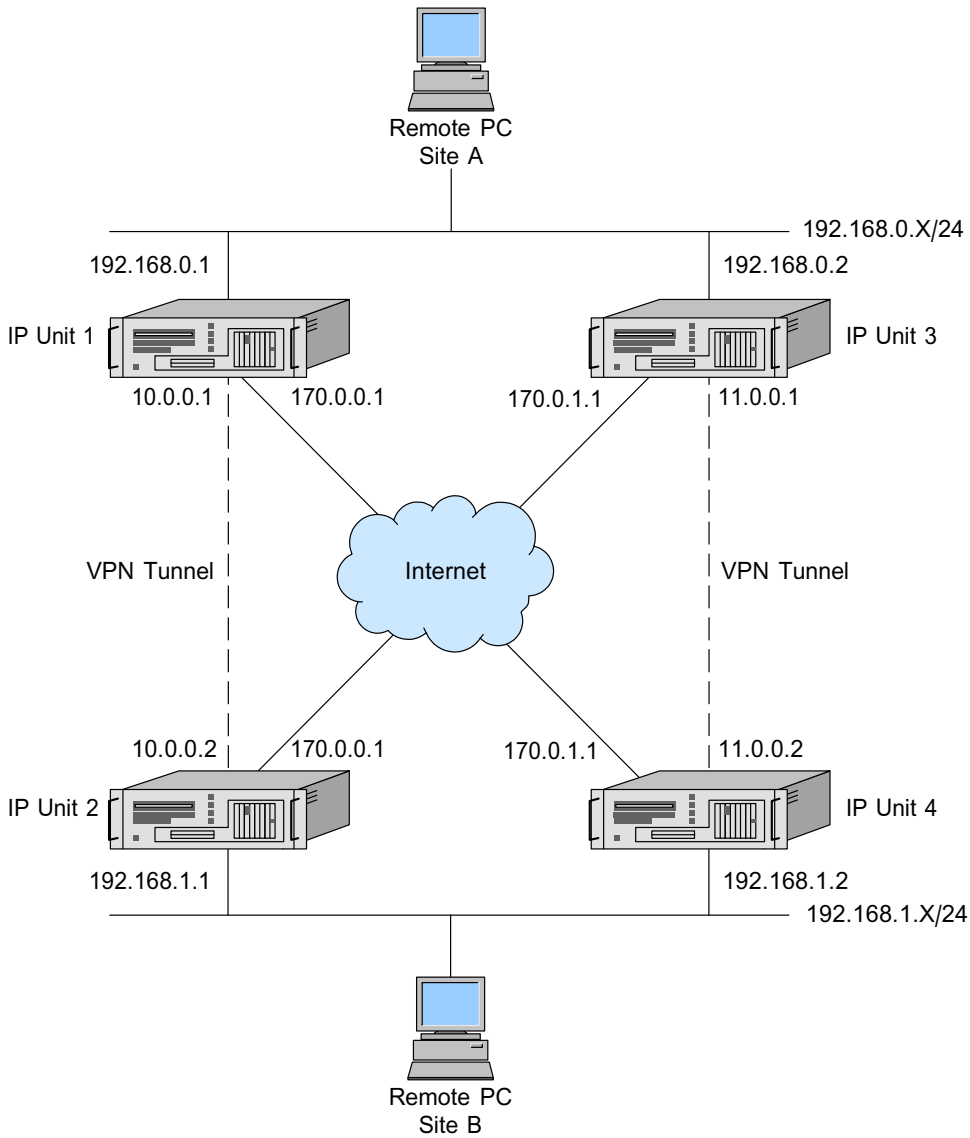


Figure 11. Example of network configuration for HA GRE tunnel

Note

Step 1 below must be completed first. Steps 2 through 4 below may be completed in any order.



Steps

- 1. Perform the steps as presented in the GRE tunnel example section. In order to create an HA GRE tunnel, we need to create multiple tunnels and in two directions. This example requires repeating steps 7 through 10 of the GRE tunnel example four times as follows:**

- Configuring from IP Unit 1 to IP Unit 2:
Enter **10.0.0.2** in the **Local Address** edit box.
Enter **10.0.0.1** in the **Remote Address** edit box.
Enter **171.0.0.1** in the **Local Endpoint** edit box.
Enter **170.0.0.1** in the **Remote Endpoint** edit box.
- Configuring from IP Unit 2 to IP Unit 1:
Enter **10.0.0.2** in the **Local Address** edit box.
Enter **10.0.0.1** in the **Remote Address** edit box.
Enter **171.0.0.1** in the **Local Endpoint** edit box.
Enter **170.0.0.1** in the **Remote Endpoint** edit box.
- Configuring from IP Unit 3 to IP Unit 4:
Enter **11.0.0.1** in the **Local Address** edit box.
Enter **11.0.0.2** in the **Remote Address** edit box.
Enter **170.0.0.1** in the **Local Endpoint** edit box.
Enter **171.0.0.1** in the **Remote Endpoint** edit box.
- Configuring from IP Unit 3 to IP Unit 4:
Enter **11.0.0.2** in the **Local Address** edit box.
Enter **11.0.0.1** in the **Remote Address** edit box.
Enter **171.0.0.1** in the **Local Endpoint** edit box.
Enter **170.0.0.1** in the **Remote Endpoint** edit box.

- 2. OSPF provides redundancy in case a tunnel goes down. OSPF detects when the router at the other end of an HA GRE tunnel is no longer reachable and then obtains a new route using the backup HA GRE tunnel and forwards the packets to the backup router. Perform the steps as presented in the Configuring OSPF example section. For this example, enable OSPF using the following interface values:**

IP Unit 1: 10.0.0.1 and 192.168.0.1

IP Unit 2: 10.0.0.2 and 192.168.1.1

IP Unit 3: 11.0.0.1 and 192.168.0.2

IP Unit 4: 11.0.0.2 and 192.168.1.2

Use `iclid` to show all OSPF neighbours. Each router should show two neighbours and also show that the best route to the destination network is through the corresponding HA GRE tunnel.

- VRRP-v2 provides redundancy in case one of the routers is lost. Perform the steps as presented in the Creating a Virtual router for an interface's addresses in VRRPv2 section. Use the following values to configure VRRP-v2:**

IP Unit 1: Enable VRRP on 192.168.0.1 with 192.168.0.2 as a backup

IP Unit 2: Enable VRRP on 192.168.1.1 with 192.168.1.2 as a backup

IP Unit 3: Enable VRRP on 192.168.0.2 with 192.168.0.1 as a backup

IP Unit 4: Enable VRRP on 192.168.1.2 with 192.168.1.1 as a backup

- HA GRE tunnels work by encapsulating the original packet and resending the packet through the router. The first time the router sees the packet, it has the original IP header; the second time, the packet has the end points of the tunnels as the src and dst IP addresses.**

The router needs to be configured to accept all packets with the original IP header so the encapsulation can take place. An encrypt rule is then defined to encrypt those packets matching the tunnel endpoints.

32 DVMRP tunnel configuration example

Purpose

The example below contains one connection to the internet through an internet service provider (ISP). This ISP provides a multicast traffic tunnel. Multicast traffic uses the address space above 224.0.0.0 and below 238.0.0.0. Multicast traffic is different from unicast (point-to-point) traffic in that it is one-to-many traffic forwarded by routers.

A router forwards multicast traffic to an adjacent router only if that router has a client that accepts multicast traffic. Nokia network application platforms (NAPs) require distance vector multi-protocol routing (DVMRP) to be enabled on the interfaces to which you forward multicast traffic.

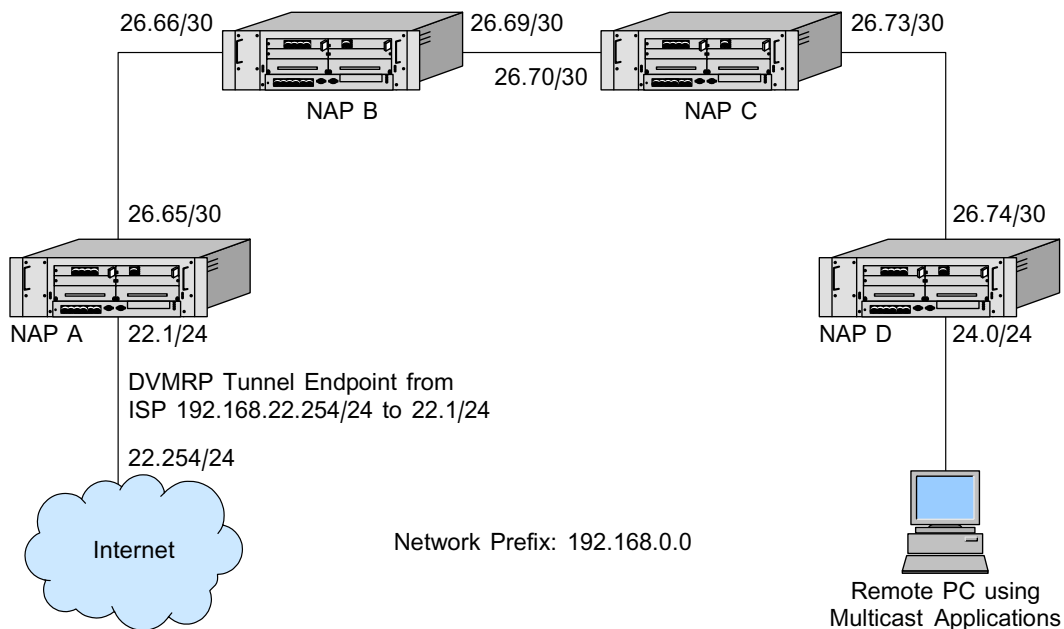


Figure 12. Example of network configuration for DVMRP tunnels



Steps

1. **Initiate a voyager session to NAP A.**
In this example, we use NAP A as the starting point.
2. **Click Config on the home page.**
3. **Click the *Interfaces* link.**
4. **Click Tunnels in the Physical column.**
5. **From the pulldown menu in the Create a New Tunnel Interface with Encapsulation, select DVMRP.**
6. **Click Apply.**

Expected outcome

Each time you select a tunnel encapsulation and click **Apply**, a new tunnel appears in the table.

7. **Click the logical interface name in the Interface column of the Logical Interfaces table.**

For example, `tun0c1`.

Expected outcome

This takes you to the interface page for the specified tunnel.

8. **Enter the following in the Local IP Address box: 192 . 168 . 22 . 1.**
9. **Enter the following in the Remote IP Address edit box: 192 . 168 . 22 . 254.**
10. **(Optional) Change the interface's logical name to a more meaningful one by typing the preferred name in the Logical Name edit box.**
11. **Click Apply.**
12. **To make your changes permanent, click Save.**

Note

Steps 17 through 21 require that you use the *Routing Configuration* page by first doing the following:

13. **Click Config on the home page.**
14. **Click the *DVMRP* link in the Routing configuration section.**
15. **For each interface you want to configure for DVMRP, click the On radio button for the interface.**
16. **Click Apply.**
17. **(Optional) Define the time-to-live (TTL) threshold for the multicast datagram.**

Enter it as follows in the **Threshold** edit box: **128**

We use 128 for the purpose of broadcasting. A 128 TTL is defined as internet broadcast.

18. **(Optional) Define the cost of the tunnel. Enter this cost in the Metric edit box.**

This shows the route preference. Leave this as the default unless there are many other multicast tunnels present in your network.

19. **Click Apply.**
20. **Perform steps 1 through 13 with addresses reversed on the exit point for the multicast tunnel.**

In this example, the ISP has already done this for us.

21. **Ensure that DVMRP is running on all interfaces (Ethernet, ATM, FDDI) on which the multicast is to be received.**

For more information, see *Configuring DVMRP*.

33 Configuring ARP



Steps

1. **Go to the ARP Configuration page of the Voyager.**
 - a. Click **Config** on the Voyager home page.
 - b. Click the *ARP* link under the *Interfaces* section.

2. **Enter the keep time (in seconds).**

Enter the keep time (in seconds) in the **Keep Time** field in the **Global ARP Settings** section.

Further information

Keep time specifies the time, in seconds, to keep resolved dynamic ARP entries. If the entry is not referenced and not used by traffic after the given time elapses, the entry is removed. Otherwise, a request is sent again to verify the MAC address. The range of the Keep Time value is 1 to 86400 seconds with a default of 14400 seconds (4 hours).

3. **Enter the retry limit.**

Enter the retry limit in the **Retry Limit** field in the **Global ARP Settings** section.

Further information

Retry limit specifies the number of times to retry ARP requests until holding off requests for the holdoff time, which is 20 seconds. Retry requests occur at a rate of up to once per second. The range of retry limit is 1 to 100 and the default value is 3.

4. **Click Apply.**
5. **To make your changes permanent, click Save.**

Further information

See *Creating static ARP entries*, *Creating proxy ARP entries* and *Viewing dynamic ARP entries*

34 Creating static ARP entries

Before you start

In order to create ARP entries, you need to be on the ARP configuration page:

1. Click **Config** on the Voyager home page.
2. Click the *ARP* link under the *Interfaces* section.



Steps

1. **Enter the new IP address.**

Enter the IP address of the static ARP entry in the **IP Address** field in the *Add a New Static ARP Entry* section.

2. **Enter the MAC address.**

Enter the MAC address corresponding to the IP address in the **MAC Address** field in the same table.

3. **Click Apply.**

Expected outcome

A new static ARP entry appears in the **Static ARP Entries** table.

4. **To make your changes permanent, click Save.**

Further information

See *Configuring ARP* and *Removing ARP entries*

35

Creating proxy ARP entries

Purpose

A proxy ARP entry makes this system respond to ARP requests for a given IP address received through any interface. Proxy ARP entries will not be used by this system when forwarding packets.

Before you start

In order to create ARP entries, you need to be on the ARP configuration page:

1. Click **Config** on the Voyager home page.
2. Click the *ARP* link under the *Interfaces* section.



Steps

1. **Enter the new IP address.**

Enter the IP address of the proxy ARP entry in the **IP Address** field in the **Add a New Proxy ARP Entry** section.

2. **Select the MAC address.**

In the **Interface** field of the **Add a new Proxy ARP Entry** section, select the interface whose MAC address is returned in ARP replies. Selecting **User-Defined MAC Address** allows you to specify an arbitrary MAC address for the entry.

3. *If* You selected **User-Defined MAC Address** as the MAC address.

Then

Enter the MAC address.

Enter the MAC address corresponding to the IP address in the **MAC Address** edit box in the **Proxy ARP Entries** table.

4. **Click Apply.**

Expected outcome

A new proxy ARP entry appears in the **Proxy ARP Entries** table.

5. **To make your changes permanent, click Save.**

Further information

See *Configuring ARP* and *Removing ARP entries*

36

Viewing dynamic ARP entries



Steps

1. **Go to the ARP Configuration page of the Voyager.**
 - a. Click **Config** on the Voyager home page.
 - b. Click the *ARP* link under the *Interfaces* section.
2. **Display the dynamic ARP entries.**

Click the *Display or Remove Dynamic ARP Entries* link to display the dynamic ARP entries.

37 Removing ARP entries



Steps

1. **Go to the ARP Configuration page of the Voyager.**
 - a. Click **Config** on the Voyager home page.
 - b. Click the *ARP* link under the *Interfaces* section.
2. *If you are removing some of the dynamic ARP entries*

Then

Display the dynamic ARP entries.

Click the *Display or Remove Dynamic ARP Entries* link to display the dynamic ARP entries.

3. *If you want to remove all dynamic ARP entries*

Then

Click Flush.

Else

Select the entries you want to delete.

Click the check box in the **Delete** column next to the ARP entries you want to delete. Click **Apply**.

38 Configuring ARP for ATM interfaces



Steps

1. **Go to the ARP Configuration page of the Voyager.**
 - a. Click **Config** on the Voyager home page.
 - b. Click the **ARP** link under the *Interfaces* section.

2. **Enter the keep time (in seconds).**

Enter the keep time (in seconds) in the **Keep Time** field in the **Global InATMARP Settings** section.

Further information

Keep time specifies time, in seconds, to keep resolved dynamic ATM ARP entries. The range of Keep Time value is 1–900 seconds. The default value is 900 seconds (15 minutes).

3. **Enter the timeout (in seconds).**

Enter the timeout in the **Timeout** field in the **Global InATMARP Settings** section.

Further information

Timeout specifies an InATMARP request retransmission interval in seconds. Voyager enforces that the timeout must be less than a third of Keep Time. The Range of Timeout value is 1-300 with a default value of five seconds.

4. **Enter the retry limit.**

Enter the retry limit in the **Retry Limit** field in the **Global InATMARP Settings** section.

Further information

Retry limit specifies the number of times to retry InATMARP requests after which the Holdoff Timer is started. The range of Retry Limit value is 1–100 with a default value of 5.

5. Enter the holdoff time (in seconds).

Enter the holdoff time in the **Holdoff Time** field in the **Global InATMARP Settings** section.

Further information

Holdoff time specifies time, in seconds, to hold off InATMARP requests after the maximum number of retries. The range of Holdoff Time value is 1–900 seconds (15 minutes) with a default value of 60 seconds (one minute).

6. Click Apply.

7. To make your changes permanent, click Save.

Further information

The InATMARP protocol is used for finding a mapping from IP addresses to ATM PVCs in a logical IP subnet (LIS) on top of an ATM network.

39

Creating static ATM ARP entries

Before you start

Note

Whenever static ATM ARP entries are applied, dynamic entries are no longer updated; therefore, new neighbors cannot be seen via a dynamic InATMARP mechanism.

In order to create ATM ARP entries, you need to be on the ARP Entry page of the appropriate ATM logical interface:

1. Click **Config** on the Voyager home page.
2. Click the *Interfaces* link.
3. Click the link of the correct ATM logical interface in the **Logical** column.
4. Click the *ATM ARP Entries* link.



Steps

1. **Enter the new IP address.**

Enter the IP address of the static ATM ARP entry in the **IP Address** field in the *Add a New Static ATM ARP Entry* section.

The IP address has to belong to the subnet of the logical ATM interface.

2. **Enter the VPI/VCI number of the PVC.**

Enter the VPI/VCI number of the corresponding PVC in the **VPI/VCI** field in the same table.

The VCI has to be one of the VCI:s configured for the interface.

3. Click Apply.**Expected outcome**

A new static ATM ARP entry appears in the **Static ATM ARP Entries** table. The IP datagrams destined to the IP address of the entry will be sent to the PVC specified in the entry.

4. To make your changes permanent, click Save.**Further information**

See *Configuring ARP for ATM interfaces* and *Removing ATM ARP entries*

40 Removing ATM ARP entries



Steps

1. **Go to the ARP Entry page of the correct ATM interface.**
 - a. Click **Config** on the Voyager home page.
 - b. Click the *Interfaces* link.
 - c. Click the link of the correct ATM logical interface in the **Logical** column.
 - d. Click the *ATM ARP Entries* link.

2. **Select the ATM ARP entries you want to delete.**

Click the check box in the **Delete** column next to the ATM ARP entries you want to delete.

3. **Click Apply.**

Further information

Note

Deleting a dynamic entry triggers a transmission of an InATMARP request on the PVC. If the remote end responds and its IP address has not changed, a new dynamic ATM ARP entry identical to the deleted one appears in the table immediately.

4. **To make your changes permanent, click Save.**