

NOKIA

Router services 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	Bootstrap protocol (Bootp) relay	5
2	Enabling Bootp relay on an interface	7
3	Disabling Bootp relay on an interface	9
4	IP broadcast helper	11
5	Configuring IP helper services	13
6	Enabling Forward Nonlocal	15
7	Disabling IP helper services	17
8	Router discovery	19
9	Enabling router discovery services	21
10	Disabling router discovery services	23
11	Virtual router redundancy protocol (VRRP)	25
12	Creating a virtual router for an interface's addresses in VRRPv2	31
13	Creating a virtual router to back up another VRRP router's addresses in VRRPv2	33
14	Enabling coldstart delay	37
15	Enabling accept connections to VRRP IPs	39
16	Setting virtual MAC (VMAC) address for virtual router	41
17	Removing virtual routers in VRRPv2	43
18	Changing the IP address list of virtual routers in VRRPv2	45
19	Changing the priority of virtual router in VRRPv2	47
20	Changing the hello interval of a virtual router in VRRPv2	49
21	Changing authentication method and password in VRRPv2	51
22	Creating a virtual router in monitored circuit mode	53
23	Removing a virtual router in monitored circuit mode	55

- 24 Changing the priority of a virtual router in monitored circuit mode 57**
- 25 Changing the hello interval of a virtual router in monitored circuit mode 59**
- 26 Changing the IP address list of a virtual router in monitored circuit mode 61**
- 27 Changing the list of monitored interfaces in monitored circuit mode 63**
- 28 Changing authentication method and password in monitored circuit mode 65**
- 29 Monitoring VRRP 67**
- 30 NTP 69**
- 31 Configuring NTP 71**
- 32 Configuring NTP IPv6 75**

1 Bootstrap protocol (Bootp) relay

Bootp relay extends bootstrap protocol (Bootp) and dynamic host configuration protocol (DHCP) operation across multiple hops in a routed network. In standard Bootp, all interfaces on a LAN are loaded from a single configuration server on the LAN. Bootp relay allows configuration requests to be forwarded to and serviced from configuration servers located outside the single LAN. Bootp relay has the following advantages over standard Bootp.

- It makes it possible to bootstrap load from redundant servers by allowing multiple servers to be configured for a single interface. If one of the redundant configuration servers is unable to perform its job, another will take its place.
- It provides load balancing by allowing different servers to be configured for different interfaces instead of requiring all interfaces to be loaded from a single configuration server.
- It allows more centralized management of the bootstrap loading of clients. This becomes more important as the network becomes larger.

IPSO's implementation of Bootp relay is compliant with RFC 951, RFC 1542, and RFC 2131. Bootp relay supports Ethernet and IEEE 802 LANs using canonical MAC byte ordering.

When an interface configured for Bootp relay receives a boot request, it forwards the request to all the servers in its server list. It does this after waiting a specified length of time to see if a local server answers the boot request. If a primary IP is specified, it stamps the request with that address, otherwise it stamps the request with the lowest numeric IP address specified for the interface.

You can use Voyager to enable Bootp relay on each interface. If the interface is enabled for relay, you can set up a number of servers to which to forward Bootp requests. Enter a new IP address in the NEW SERVER edit box for each server. To delete a server, turn it off.

You can set the number of seconds to wait for a local configuration server to answer the boot request before forwarding the request through the interface. Enter the number of seconds to wait in the WAIT TIME edit box. Set the wait time to be of sufficient length to allow the local configuration server to respond before the request is forwarded. If there is no local server, set the time to zero.

If you enter an IP address in the PRIMARY IP edit box, all Bootp requests received on the interface will be stamped with this gateway address. This can be useful on interfaces with multiple IP addresses (aliases).

2

Enabling Bootp relay on an interface



Steps

1. Click **Config** on the home page.
2. Click the *Bootp Relay* link in the *Router Services* section.
3. Locate the interface on which you want to enable **Bootp**.
4. Click the **On** radio button for that interface.
5. Click **Apply** to enable the interface.
6. (Optional) Enter the minimum client-elapsed time (in seconds) before forwarding a **Bootp** request in the **Wait Time** edit box.
7. (Optional) Enter the IP address to use as the **Bootp** router address in the **Primary IP** edit box.
8. (Optional) Enter the IP address of the **BOOTP/DHCP** configuration server to which to relay **Bootp** requests in the **New Server** edit box.
9. Click **Apply**.
10. If you want to relay **Bootp** requests to more than one server
Then
Repeat steps 8 and 9.
11. To make your changes permanent, click **Save**.

Further information

See *Disabling Bootp relay on an interface*

3

Disabling Bootp relay on an interface

Before you start

Note

When you disable Bootp relay on an interface, the **Wait Time**, **Primary IP**, and **New Server** fields disappear, but the parameters are still stored in the system.



Steps

1. Click **Config** on the home page.
2. Click the **Bootp Relay** link in the **Router Services** section.
3. Locate the Bootp relay interface to be disabled.
4. Click the **Off** radio button for the interface you want to disable.
5. Click **Apply** to disable the interface.

Expected outcome

The Bootp relay parameters no longer appear.

Further information

When you click the **On** button in the **BOOTP/DHCP Relay Interfaces** field, then the **Apply** button, the Bootp relay parameters will appear again.

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

4

IP broadcast helper

IP broadcast helper is a form of static addressing that uses directed broadcasts to forward local and all-nets broadcasts to desired destinations within the internetwork.

It is not possible to pass BOOTPUDP packets using the IP broadcast helper (UDP port 67). The reason for this is that the BOOTP functionality on a router is different from generic UDP packet forwarding to a specified IP address.

While the IP broadcast helper simply forwards the UDP packet to the IP address without modification, the BOOTP implementation is more complex. Below is a quick explanation of BOOTP forwarding in a router:

Client--> Sends broadcast bootp packet ---->[router] ---->Sends modified packet to server

The router will modify the packet by inserting its IP address in the giaddr field of the BOOTP packet (this is needed for the server to identify the network where the packet originated).

5

Configuring IP helper services



Steps

1. Click **Config** on the home page.
2. Click the **IP Broadcast Helper** link in the **Router Services** section.
3. Click the **On** radio button for each interface you want to support **IP Helper** service. Click **Apply**.
4. (Optional) If you want to add a new **UDP Port** to the helper services, enter the new **UDP port number** in the **New UDP Port** edit box. Click **Apply**.
5. (Optional) If you want to add a new server to a **UDP port**, enter the new server **IP address** in the **New Address For UDP Port X** edit box. Click **Apply**.
6. Verify that each interface, **UDP port**, or server is enabled (**ON** radio button checked) or disabled (**OFF** radio button checked) for **IP helper** support according to your needs.
7. To make your changes permanent, click **Save**.

6

Enabling Forward Nonlocal

Purpose

The Forward Nonlocal feature allows you to forward packets that are not originated by a source that is directly on the receiving interface. When you enable Forward Nonlocal, it applies to all interfaces that are running the IP Helper service.



Steps

1. **Click Config on the home page.**
2. **Click the *IP Broadcast Helper* link in the *Router Services* section.**
3. **Click the Enabled radio button in the Forward Nonlocal field.**

Note

The default is disabled, which requires that packets be generated by a source directly on the receiving interface to be eligible for relay.

4. **Click Apply.**
5. **Click Save to make your change permanent.**
6. **To disable the Forward Nonlocal feature if you have enabled it, click the Disabled radio button in the Forward Nonlocal field.**
7. **Click Apply.**
8. **Click Save to make your change permanent.**

7

Disabling IP helper services



Steps

1. Click **Config** on the home page.
2. Click the *IP Broadcast Helper* link in the *Router Services* section.
3. Click the **Off** radio button for each interface you want to disable for **IP Helper** service. Click **Apply**.
4. Click the **Off** radio button for each **UDP** port you want to disable for **IP Helper** service. Click **Apply**.
5. Click the **Off** radio button for each server you want to disable for **IP Helper** service. Click **Apply**.
6. To make your changes permanent, click **Save**.

8

Router discovery

The ICMP router discovery protocol is an IETF standard protocol used to inform hosts of the existence of routers. It is intended to be used instead of having hosts wiretap routing protocols such as RIP. It is used in place of, or in addition to, statically configured default routes in hosts.

The ICMP router discovery service provides a mechanism for hosts attached to a multicast or broadcast network to discover the IP addresses of their neighboring routers.

Note

Only the server portion of the router discovery protocol is supported.

Router discovery server

The router discovery server runs on routers and announces their existence to hosts. It does this by periodically multicasting or broadcasting a router advertisement to each interface on which it is enabled. These advertisements contain a list of all the router addresses on a given interface and their preference for use as a default router.

Initially, these router advertisements occur every few seconds, then fall back to every few minutes. In addition, a host may send a router solicitation, to which the router will respond with a unicast router advertisement, unless a multicast or broadcast advertisement is due momentarily.

Each router advertisement contains an advertisement lifetime field indicating for how long the advertised addresses are valid. This lifetime is configured such that another router advertisement will be sent before the lifetime has expired. A lifetime of zero indicates that one or more addresses are no longer valid.

On systems supporting IP multicasting, the router advertisements are sent by default to the all-hosts multicast address 224.0.0.1. However, the use of broadcast may be specified. When router advertisements are being sent to the all-hosts multicast address, or an interface is configured for the limited-broadcast address 255.255.255.255, all IP addresses configured on the physical interface are included in the router advertisement. When the router advertisements are being sent to a net or subnet broadcast, only the address associated with that net or subnet is included.

9

Enabling router discovery services



Steps

1. Click **Config** on the home page.
2. Click the **Router Discovery** link in the **Router Services** section.
3. Click the **On** radio button for each interface you want to support router discovery service.

4. Click **Apply**.

5. **(Optional) Enter the minimum advertisement interval for each enabled interface in the Minimum Advertisement Interval edit box.**

Range: Between 3 seconds and the value in the Maximum advertisement interval field.

Default: 0.75 times the value in the Maximum advertisement interval field.

6. **(Optional) Enter the maximum advertisement interval for each enabled interface in the Maximum Advertisement Interval edit box. Click Apply.**

Range: 4-1800.

Default: 600.

7. **(Optional) Enter the lifetime of advertisement packets for each enabled interface in the Advertisement Lifetime edit box. Click Apply.**

Range: Between the value in the Maximum advertisement interval field and 9000 seconds

Default: 3 times the values in the Maximum advertisement interval field.

8. (Optional) Specify whether or not an IP address should be advertised in the Router Advertisement packets.

The default is YES. To disable this feature and specify not to advertise an IP address, click the **No** radio button in the **Advertise Address** field and then click **Apply**.

Note

This option applies to each address on the interface and not to the interface itself.

9. (Optional) Specify the preferability of an IP address as a default router address, relative to other addresses on the same subnet.

You can also make an IP address ineligible as a default router address.

- a. Click the **Ineligible** radio button to remove an IP address as a possible default router address.

The default is ELIGIBLE. Enter a value to indicate the level of preference for the IP address as a default router address in the edit box below the **Eligible** radio button. The default is 0.

- b. Click **Apply**.
-

Note

This option applies to each address on the interface and not to the interface itself.

10. To make your changes permanent, click Save.

10 Disabling router discovery services



Steps

1. Click **Config** on the home page.
2. Click the **Router Discovery** link in the **Router Services** section.
3. Click the **Off** radio button for each interface you want to disable support for router discovery service. Click **Apply**.
4. To make your changes permanent, click **Save**.

11

Virtual router redundancy protocol (VRRP)

Virtual router redundancy protocol (VRRP) provides dynamic fail-over of IP addresses from one router to another in the event of failure. It is used on shared media where end hosts are configured with a static default route. In this environment, normally the loss of the default router results in a catastrophic event, isolating all end hosts that are unable to detect any alternate path that may be available. Using VRRP, a router can automatically assume responsibility for forwarding IP traffic sent to the default router's address, should the default router fail. This allows a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end host.

Virtual routers

To back up a default router using VRRP, a virtual router must be created for it. A virtual router consists of a unique virtual router ID (VRID), and the default router's IP address(es) on the shared LAN.

The virtual router is created on the default router by specifying the router's interface to the shared LAN and by specifying the VRID by which this router's addresses will be identified in the LAN. The default router's IP addresses are added to the virtual router automatically.

Once a virtual router has been created on the default router, other routers can be configured as backup routers. This is done by configuring the default router's virtual router information (its VRID and IP addresses) on each of the backup routers. They will then use VRRP to take over the default router's addresses, should it fail.

Priority

Priority provides a way to prefer one router in favor of another during contention for a failed router's addresses. If more than one backup router is configured for a virtual router, only one of them will assume forwarding responsibility for the failed default router. The routers' relative priorities are used by VRRP to determine which router that will be.

- Priority is a numeric value; the higher the value, the higher the priority. If the configured priorities of two backup routers is equal, their IP addresses are used as a tiebreaker.
- The router that owns the IP addresses configured in the virtual router always has the highest priority. Once a failed router recovers, it will always reclaim responsibility for forwarding traffic sent to its own addresses.

You specify priority when configuring a router to back up another.

Hello interval

The hello interval is the time interval (in seconds) between VRRP advertisements. It also determines the fail-over interval; that is, how long it takes a backup router to take over from a failed default router.

VRRP advertisements are broadcast on the LAN by the current master of each virtual router. Backup routers listen for these advertisements and assume failure if they have not received an advertisement within three hello intervals. They then elect a new master of the virtual router, based on their relative priorities.

Authentication methods

VRRP is designed for a range of internetworking environments that may employ different security policies. The protocol includes several authentication methods to protect against attacks from remote and local networks.

Independent of any authentication type, VRRP includes a mechanism (setting TTL=255, checking on receipt) that protects against remote networks injecting VRRP packets. This limits vulnerability to local attacks.

The supported authentication methods include the following:

- No Authentication

This authentication type means that VRRP protocol exchanges are not authenticated. This method should be used only in environments where there is minimal security risk and little chance for configuration errors (e. g., two VRRP routers on a LAN).

- Simple Text Password

This authentication type means that VRRP protocol exchanges are authenticated by a simple clear-text password.

This method is useful to protect against accidental misconfiguration of routers on a LAN. It also protects against routers inadvertently backing up another router. A new router must first be configured with the correct password before it can run VRRP with another router. This type of authentication does not protect against hostile attacks where the password can be learned by a node snooping VRRP packets on the LAN. The simple text authentication combined with the TTL check makes it difficult for a VRRP packet being from another LAN to disrupt VRRP operation.

This type of authentication is recommended when there is minimal risk of nodes on a LAN actively disrupting VRRP operation.

The authentication method selected must be the same for all routers running VRRP on the shared media network.

Monitored circuit

Running VRRP in a static routed environment can lead to a “black hole” failure scenario. If a link on the VRRP master fails, it may accept packets from an end host but be unable to forward them to destinations reached via the failed link. This creates an unnecessary black hole for those destinations if there is an alternate path available via the VRRP backup.

The VRRP monitored circuit feature allows the virtual router master election priority to be made dependent on the current state of the access link. With proper selection of base priority and dynamic priority update based on interface status, the virtual router forwarding responsibility can be made to gracefully failover due to interface failure on the master router.

In order to utilize the monitored circuit feature, you must select a virtual router address that does not match an interface address or any IP address allocated to a host. The ICMP redirect messages must be disabled as well.

You can select either monitored circuit mode or VRRP v.2.

Sample configuration 1

The following figure shows a simple network with two routers implementing one virtual router, to back up a single default router.

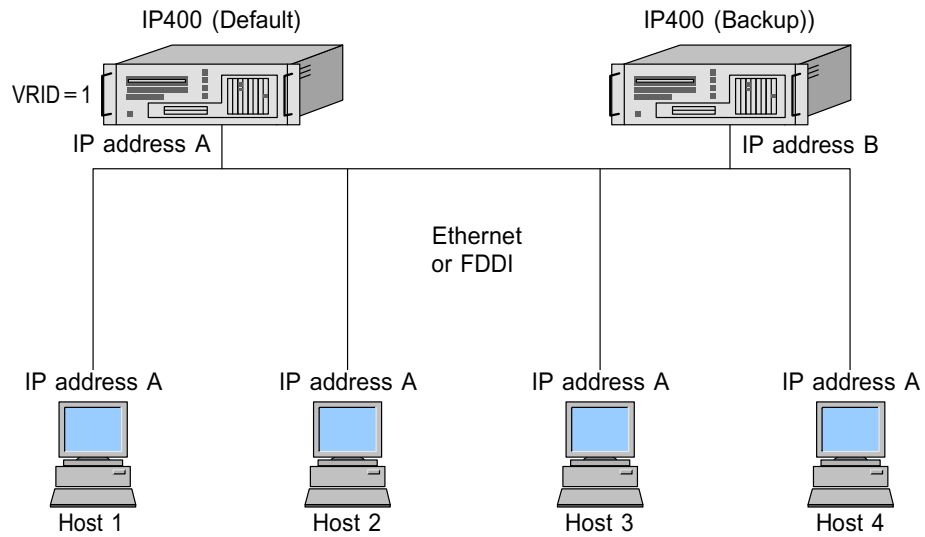


Figure 1. VRRP configuration example 1

The above configuration shows a very simple VRRP scenario. In this configuration, the end hosts install a default route to the IP address of virtual router #1 (IP A) and both routers run VRRP.

The router on the left has its address configured as virtual router #1 (VRID=1) and the router on the right is the backup for virtual router #1.

If the router on the left should fail, the other router will take over virtual router #1 and its IP addresses and provide uninterrupted service for the hosts.

Note that in this example, IP B is not backed up by the router on the left. IP B is only used by the router on the right as its interface address. In order to backup IP B, a second virtual router would have to be configured. This is shown in the third example.

Sample configuration 2

The following figure shows a network with three routers implementing one virtual router, to back up a single default router.

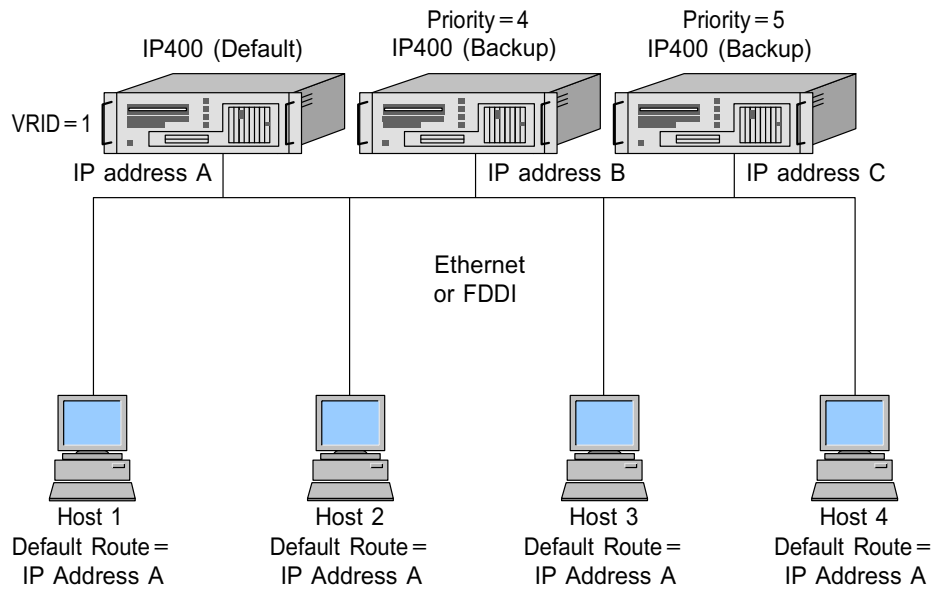


Figure 2. VRRP configuration example 2

In this configuration, the end hosts install a default route to the IP address of virtual router #1 (IP A) and all routers run VRRP. The router on the left has its address configured as virtual router #1 (VRID=1) and the other two routers are backup routers for virtual router #1, configured with different priorities. If the router on the left should fail, the other routers will use VRRP to determine which of them will take over virtual router #1 and its IP addresses. In this example, the router on the right will take over virtual router #1, as it has the higher priority. If it should also fail at some later time, the center router will take over virtual router #1. Default router service to the hosts is uninterrupted throughout.

Note that in this example, IP B and IP C are not backed up by virtual router #1. These addresses are only used by the routers as their interface addresses. In order to back up IP B and IP C, additional virtual routers would have to be configured.

Sample configuration 3

The following figure shows a configuration with two virtual routers with the hosts splitting their traffic between them. This example is common in actual practice.

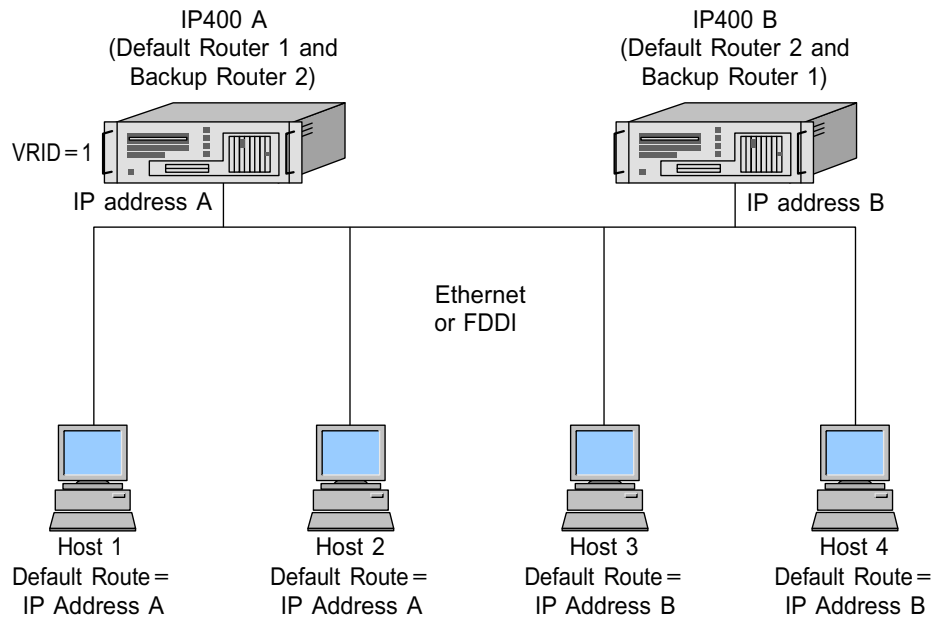


Figure 3. VRRP configuration example 3

In the above configuration, half of the hosts install a default route to virtual router #1's IP address (IP A), and the other half of the hosts install a default route to virtual router #2's IP address (IP B).

The router on the left has its address configured as virtual router #1 (VRID=1), and the router on the right has its address configured as virtual router #2. Each router is also configured as a backup router of the other. If either router should fail, the other router will take over its virtual router and IP addresses and provide uninterrupted service to both default IP addresses for the hosts. This has the effect of load balancing the outgoing traffic, while also providing full redundancy.

12

Creating a virtual router for an interface's addresses in VRRPv2

Purpose

You must configure a virtual router on an interface to enable other routers to back up its address(es).



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the *Router Services* section.**
3. **Click the VRRPV2 radio button next to the interface for which you want to enable VRRP.**
4. **Click Apply.**
5. **Enter a number for the VRID in the Own VRID edit box.**

Note

This value is used by other routers on the LAN to back up this router's addresses. It must not be used by any other routers on the LAN to configure VRRP for their own addresses.

6. **Click Apply.**
7. **(Optional) Enter a number in the Hello Interval edit box, and click Apply.**
8. **Click the None or Simple radio button to select the authentication method to be used by VRRP on this LAN.**

Note

The value in this field must be the same for all routers running VRRP on this interface's LAN.

9. **Click Apply.**
10. *If you selected **Simple***

Then

Enter the authentication password string in the Password edit box, and click Apply.

Note

The value in this field must be the same for all routers running VRRP on this interface's LAN.

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

13

Creating a virtual router to back up another VRRP router's addresses in VRRPv2

Purpose

Note

Do not turn on the virtual router redundancy protocol (VRRP) backup router before the VRRP master router is configured. This will lead to a service outage because the VRRP backup router will take over the IP address while the master is still active with that IP address. To configure the master router, see *Creating a virtual router for an interface's addresses in VRRPv2*.

You can configure virtual routers to back up the addresses of other routers on a shared media network.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the Router Services section.**
3. **Click the VRRPV2 radio button next to the interface for which you want to enable VRRP.**
4. **Click Apply.**
5. **Enter the remote router's VRID in the Backup Router With VRID edit box.**

Note

This value must be the same VRID as that on the virtual router created on the remote router to back up its addresses.

6. Click Apply.**Expected outcome**

Additional fields will appear in the table, allowing you to enter information about the remote router.

7. (Optional) Enter a number in the Priority edit box, and click Apply.

This number indicates the preference of this router relative to the other routers configured to back up the virtual router. The higher the number, the higher the preference.

8. (Optional) Enter a number in the Hello Interval edit box, and click Apply.**9. Enter an IP address in the BackupAddress edit box.**

Note

The IP address is the address of the default router this system will back up. It must be in the same IP subnet as one of the addresses on this interface.

10. Click Apply.**11. If the router you are backing up has more than one IP address**

Then

Repeat step 9.

12. Click the None or Simple radio button to select the authentication method to be used by VRRP on this LAN.

Note

The authentication type and the simple password must be the same for all VRRP routers on a LAN.

13. Click Apply.

14. *If you selected **Simple***

Then

Enter the authentication password string in the Password edit box, and click Apply.

Note

The value in this field must be the same for all routers running VRRP on this interface's LAN.

15. To make your changes permanent, click Save.

14 Enabling coldstart delay

Purpose

This feature allows you to specify a delay after system coldstart before transitioning any configured VRRP virtual router out of the init state.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the Router Services section.**
3. **Enter a value (in seconds) in the Coldstart Delay edit box.**

You can enter up to 3600.

4. **To disable Coldstart Delay, enter 0 in the Coldstart Delay edit box.**

This value is also the default.

5. **Click Apply.**
6. **Click Save to make your changes permanent.**

15 Enabling accept connections to VRRP IPs

Purpose

This feature allows you to accept and respond to IP packets destined to an adopted VRRP IP address. The VRRP protocol specifies not to accept or respond to such IP packets. Overriding this specification can be useful in deploying applications whose service is tied to a VRRP IP address.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the *Router Services* section.**
3. **Click the Enabled radio button to accept connections to VRRP IPs.**
4. **To disable this option, if you have enabled it, click the Disabled radio button.**

The default is Disabled.

5. **Click Apply.**
6. **Click Save to make your changes permanent.**

16

Setting virtual MAC (VMAC) address for virtual router

Purpose

This feature allows you to set a virtual MAC address for a virtual router by using one of three options. The implementation continues to support the default selection of a VMAC through the method outlined in the VRRP protocol specification. All three modes are useful for virtual LAN deployments, which forward traffic based on the VLAN address and destination MAC address.

- The Interface mode selects the interface hardware MAC address as the VMAC.
- In the Static mode, you specify fully the VMAC address.
- In the extended mode, the system dynamically calculates three bytes of the interface hardware MAC address to extend its range of uniqueness.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the Router Services section.**
3. **Set the VMAC option for an interface on which you enable VRRP or Monitored Circuit:**
 - a. To enable VRRP, click the **VRRPV2** radio button next to the interface for which you want to enable VRRP, and then click **Apply**.
 - b. To specify the virtual router ID for the virtual router used to back up the local interface's address(es), enter a value between **1** and **255** in the **Own VRID** edit box. Click **Apply**.
 - c. To specify the virtual router ID for the virtual router used to back up another system's IP address(es), enter a value between **1** and **255** in the **Backup RouterWith VRID** edit box. Click **Apply**.
A **Backup Address** edit box appears that allows you to add an IP address for this virtual router.

- d. To enable Monitored Circuit, click the **Monitored Circuit** radio button next to the interface for which you want to enable Monitored Circuit, and then click **Apply**.
 - e. To specify the virtual router ID for the virtual router to be used to back up the local interface's address(es), enter a value between **1** and **255** in the **Own VRID** edit box. Click **Apply**.
 - f. Enter the IP address you want to assign to the virtual router back up in the **Backup Address** edit box. Click **Apply**.
-

Note

The IP address(es) associated with the monitored circuit virtual router must not match the real IP address of any host or router on the interface's network.

4. Set a VMAC address.

Click the **VMAC Mode** drop-down window and select either **Interface**, **Static**, or **Extended**.

VRRP is the default.

5. If you selected **Static**

Then

Enter the VMAC address that you want to use in the Static VMAC edit box.

6. Click **Apply**.

7. Click **Save to make your changes permanent**.

17 Removing virtual routers in VRRPv2

Purpose

When you disable a virtual router, the VRRP operation terminates, and the configuration information no longer displays in the browser. Fail-over of the default router will no longer occur.

Before you start

When disabling a virtual router, you must first remove the VRRP configuration for that virtual router from all of the backup routers.

You must not delete the virtual router on the default router first, as it will stop sending VRRP advertisements. This will result in the backup routers assuming the default router has failed, and one of them will adopt the default router's addresses automatically. This will result in two routers having the default router's addresses configured.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the Router Services section.**
3. **Locate the virtual router you want to remove.**

You can locate virtual router information by using the VRID value displayed in the **Router With VRID** field.

- a. To locate a virtual router used to back up an interface's addresses, find the matching VRID displayed in the **Own VRID** field.
 - b. To locate a virtual router used to back up another router's addresses, find the matching VRID displayed in the **Router With VRID** field.
4. **Click the Off radio button in the Router With VRID field to remove the virtual router.**
 5. **Click Apply.**

Expected outcome

All the information about the virtual router will disappear from the table.

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

18

Changing the IP address list of virtual routers in VRRPv2

Purpose

A virtual router that is configured for an interface contains the IP address of that interface. If IP addresses are added to or removed from the interface, they will automatically be added to or removed from the virtual router for the interface.

Virtual routers are used to back up other routers' addresses; however, they must be updated manually whenever the IP addresses of the other routers change.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the Router Services section.**
3. **Locate the interface and virtual router with the IP address you want to change.**

You can locate the virtual router information using the VRID value displayed in the **RouterWith VRID** field.

4. **To remove an IP address from the list, click the Off radio button that corresponds to the address.**
5. **Click Apply.**
6. **To add an IP address to the list, enter the IP address in the Backup Address edit box.**

Note

The IP address is the address of the default router this system will back up. It must be in the same IP subnet as one of the addresses on this interface.

7. **Click Apply.**
8. **To make your changes permanent, click Save.**

19

Changing the priority of virtual router in VRRPv2

Purpose

The priority determines which backup router takes over when the default router fails. Higher values equal higher priority.



Steps

1. Click **Config** on the home page.
2. Click the **VRRP** link in the *Router Services* section.
3. Locate the interface and virtual router with the priority you want to change.

You can locate the virtual router information using the VRID value displayed in the **RouterWith VRID** field.

- a. To locate a virtual router used to back up an interface's addresses, find the matching VRID displayed in the **Own VRID** field.
 - b. To locate a virtual router used to back up another router's addresses, find the matching VRID displayed in the **Router With VRID** field.
4. Change the number in the **Priority** edit box.

This number indicates the preference of this router relative to the other routers configured to back up the virtual router. The higher the number, the higher the preference.

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

Further information

See *Virtual router redundancy protocol (VRRP)*

20

Changing the hello interval of a virtual router in VRRPv2



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the Router Services section.**
3. **Locate the interface and virtual router with the hello interval you want to change.**
 - a. To locate a virtual router used to back up an interface's addresses, find the matching VRID displayed in the **Own VRID** field.
 - b. To locate a virtual router used to back up another router's addresses, find the matching VRID displayed in the **RouterWith VRID** field.
4. **Change the number in the Hello Interval edit box for the matching VRID. Click Apply.**

The hello interval should be the same value on all systems with this virtual router configured.

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

21

Changing authentication method and password in VRRPv2

Purpose

The authentication method provides a simple way to avoid attacks from remote and local networks. The authentication method selected must be the same for all routers running VRRP on a shared media network.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the Router Services section.**
3. **Locate the interface with the authentication method or password you want to change.**
4. **(Optional) Click the None or Simple radio button to select the authentication method used by VRRP on this interface's LAN, and click Apply.**

The value in this field must be the same for all routers running VRRP on this interface's LAN.

5. *If you selected Simple*

Then

Enter the authentication password string in the Password edit box, and click Apply.

The value in this field must be the same for all routers running VRRP on this interface's LAN.

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

22

Creating a virtual router in monitored circuit mode



Steps

1. Click **Config** on the home page.
2. Click the **VRRP** link in the *Router Services* section.
3. Click the **Monitored Circuit** radio button next to the interface for which you want to enable **Monitored Circuit**.
4. Click **Apply**.
5. Enter the **VRID** in the **Create Virtual Router** edit box.
6. Click **Apply**.
7. Enter the **IP address** you want to assign to the virtual router back up in the **Backup Address** edit box.

Note

The IP address(es) associated with the monitored circuit virtual router must not match the real IP address of any host or router on the interface's network.

8. Click **Apply**.

Repeat steps 7 and 8 if you want to add additional IP addresses.

9. **(Optional)** Enter a number in the **Priority** edit box, and click **Apply**.

This number indicates the preference of this router relative to the other routers configured to back up the virtual router. The higher the number, the higher the preference.

10. **(Optional) Enter a number in the Hello Interval edit box, and click Apply.**
 11. **Select the interface that you want to monitor from the Monitor Interface drop-down window.**
 12. **Click Apply.**
 13. **Enter a number in the Priority Delta edit box.**
-

Note

You must select the interface you want to monitor and enter a priority delta value in order to monitor interfaces. Otherwise, an error message will be displayed.

14. **Click Apply.**
15. **Repeat steps 11 to 14 if you want to add more monitored interface dependencies.**
16. **To make your changes permanent, click Save.**

Further information

See *Virtual router redundancy protocol (VRRP)*, *Removing virtual router in monitored circuit mode* and *Changing the priority of a virtual router in monitored circuit mode*

23

Removing a virtual router in monitored circuit mode



Steps

1. Click **Config** on the home page.
2. Click the **VRRP** link in the **Router Services** section.
3. Click the **Off** radio button that corresponds to the virtual router that you want to remove. Click **Apply**.

You can locate the virtual router information using the VRID value displayed in the **Virtual Router** field.

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

24

Changing the priority of a virtual router in monitored circuit mode

Purpose

The priority determines which backup router takes over when the default router fails. Higher values equal higher priority.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the *Router Services* section.**
3. **Locate the interface and virtual router with the priority you want to change.**

You can locate the virtual router information using the VRID value displayed in the **Virtual Router** field.

4. **Change the number in the Priority edit box. Click Apply.**

This number indicates the preference of this router relative to the other routers configured to back up the virtual router. The higher the number, the higher the preference.

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

25

Changing the hello interval of a virtual router in monitored circuit mode



Steps

1. Click **Config** on the home page.
2. Click the **VRRP** link in the *Router Services* section.
3. Locate the interface and virtual router with the hello interval you want to change.
4. Change the number in the **Hello Interval** edit box for the matching **VRID**. Click **Apply**.

The hello interval should be the same value on all systems with this virtual router configured.

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

26

Changing the IP address list of a virtual router in monitored circuit mode

Purpose

Virtual routers are used to back up other routers' addresses; however, they must be updated manually whenever the IP addresses of the other routers change.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the *Router Services* section.**
3. **Locate the interface and virtual router with the IP address you want to change.**

You can locate the virtual router information using the VRID value displayed in the **Virtual Router** field.

4. **To remove an IP address from the list, click the Off radio button that corresponds to the address. Click Apply.**
5. **To add an IP address to the list, enter the IP address in the Backup Address edit box. Click Apply.**

Note

The IP address is the address of the default router this system will back up. It must be in the same IP subnet as one of the addresses on this interface.

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

27

Changing the list of monitored interfaces in monitored circuit mode



Steps

1. Click **Config** on the home page.
 2. Click the **VRRP** link in the *Router Services* section.
 3. Select the interface that you want to monitor from the **Monitor Interface** drop-down window. Click **Apply**.
 4. Enter a number in the **Priority Delta** edit box. Click **Apply**.
-

Note

You must select the interface you want to monitor and enter a priority delta value in order to monitor interfaces. Otherwise, an error message will display

5. To remove an interface from being monitored, click the corresponding **Off** radio button. Click **Apply**.
6. To change the priority delta, enter a new number in the **Priority Delta** edit box. Click **Apply**.
7. To make your changes permanent, click **Save**.

28

Changing authentication method and password in monitored circuit mode

Purpose

The authentication method provides a simple way to avoid attacks from remote and local networks. The authentication method selected must be the same for all routers running VRRP on a shared media network.



Steps

1. **Click Config on the home page.**
2. **Click the VRRP link in the Router Services section.**
3. **Locate the interface with the authentication method or password you want to change.**
4. **Click the None or Simple radio button to select the authentication method used by VRRP on this interface's LAN. Click Apply.**

The value in this field must be the same for all routers running VRRP on this interface's LAN

5. **If you selected Simple, enter the authentication password string in the Password edit box. Click Apply.**

The value in this field must be the same for all routers running VRRP on this interface's LAN.

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

29 Monitoring VRRP

Purpose

There are several tools you can use for monitoring. From Voyager, you can view the virtual router redundancy protocol (VRRP) status by performing the following steps.



Steps

1. **Click Monitor on the home page.**
2. **Click the VRRP link in the *Routing Protocols* section.**
3. **Click either the *interface* link or the *stats* link, depending on what information you want.**

You will be able to display interface information and statistics on all interfaces.

You can also view these statistics in ICLID.

Execute the following commands using ICLID. For more information on these commands, see *Displaying routing protocol information*.

```
show vrrp
```

```
show vrrp interface
```

```
show vrrp stat
```

Further information

See *Virtual router redundancy protocol (VRRP)*

30 NTP

NTP is a protocol that allows you to synchronize to UTC time by querying a server with an accurate clock. This is ideal for distributed applications that require time synchronization or analyzing event logs from a different machine.

Servers

If you configure machines as servers, you will use them to set your clock. In this mode, you are synchronizing to the server for accurate time; it does not synchronize with you. It is important that you configure several servers for redundancy.

Peers

If you configure machines as peers, they will listen to each other and move toward a common time. Peers are considered equal with each other as opposed to servers, which are considered "masters". It is important that you configure several peers so that they can decide on the right time.

NTP reference clock

You can turn on the NTP reference clock if you wish to have your server configured as a source of time information. In this mode, it is recommended that you keep the stratum value at its default (0). The stratum value tells how far away the NTP reference clock is from a valid time source.

Note

The time server begins to provide time information 10 minutes after it is configured.

Features

- Setting the time manually.
- Running NTP daemon in client mode using a specified set.

- Preferring NTP peers and/or servers over other NTP peers and/or servers.
- Enabling the NTP reference clock if an NTP peer or server is unavailable.

31

Configuring NTP

Purpose

Configuring network time protocol (NTP) determines whether the time service should be active or inactive. When NTP is active, the local clock will be synchronized as configured, and hosts will be able to set their time via this machine. If, however, you want to set the time manually, see *Setting system time*.



Steps

1. Click **Config** on the home page.
2. Click the **NTP** link in the *Router Services* section.
3. Click the **Yes** radio button in the **Enable NTP** field.
4. Click **Apply**.

Expected outcome

The NTP configuration page opens.

Note

For IPv6 Configuration, follow the steps in *Configuring NTP IPv6*, beginning from step 4.

5. Enter the new server's IP address in the **Add New Server:Address:** edit box.
6. Click **Apply**.

Expected outcome

The new server's IP address will now appear in the **NTP Servers** field. By default, this new server is enabled, v3 is selected, and the **Prefer Yes** radio button is selected. As you add other servers, you may prefer them over the initial server you configured.

Note

It is recommended that you use the default setting of v3.

7. To add another new server, repeat the previous step.

Expected outcome

The new server's IP address will appear in the **NTP Servers** field. By default, this new server is enabled, v3 is selected, and the **Prefer No** radio button is selected. If you wish to prefer this server over other servers, click the **Prefer Yes** radio button, and then click **Apply**.

8. To delete a server, click the corresponding Off radio button, and click Apply.

Expected outcome

The new server's IP address will disappear from the **NTP Servers** field.

9. (Optional) Enable the NTP reference clock by clicking the Yes radio button in the NTP Master field, and click Apply.

Expected outcome

The **Stratum** edit box and **Clock Source** drop-down window will display. By default, the Stratum value is 1, and the Clock source is set to Local Clock. It is recommended that you keep these defaults.

10. If you want to configure a new peer

Then

Enter the new peer's IP address in the Add New Peer: Address: edit box, and click Apply.

Expected outcome

The new peer's IP address will now appear in the **NTP Peers** field. By default, this new peer is enabled, v3 is selected, and the **Prefer Yes** radio button is selected. As you add other peers, you may prefer them over the initial peer you configured.

Note

It is recommended that you use the default setting of v3.

11. To add another new peer, repeat step 10.

Expected outcome

The new peer's IP address will appear in the **NTP Peers** field. By default, this new peer is enabled, v3 is selected, and the **Prefer No** radio button is selected. If you wish to prefer this peer over other peers, click the **Prefer Yes** radio button, and then click **Apply**.

12. To delete a peer, click the corresponding **Off** radio button, and click **Apply**.

Expected outcome

The new peer's IP address will disappear from the **NTP Peers** field.

13. (Optional) Enable the NTP reference clock by clicking the **Yes** radio button in the **NTP Master** field, and click **Apply**.

Note

Only enable the NTP reference clock if you cannot reach an NTP server.

Expected outcome

The **Stratum** edit box and **Clock Source** drop-down window will display. By default, the Stratum value is 1, and the Clock source is set to Local Clock. It is recommended that you keep these defaults.

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

Further information

See *Network time protocol*

32

Configuring NTP IPv6



Steps

1. Click **Config** on the home page.
2. Click the **NTP** link in the *Router Services* section.
3. Click the *NTP IPV6 Configuration* link.

Expected outcome

The NTP configuration page is displayed.

Note

NTP must be enabled to proceed further with IPv6 configuration.

4. Enter the new server's IP address in the **Add New Server: Address:** edit box.
-

Note

Use IPv6 address(es) and NTP version defaults to v4.

5. Click **Apply**.

Expected outcome

The new server's IP address will now appear in the **NTP Servers** field. By default, this new server is enabled, v4 is selected, and the **Prefer No** radio button is selected. As you add other servers, you may prefer them over the initial server you configured.

- 6. To add another new server, repeat steps 4 and 5.**

Expected outcome

The new server's IP address will appear in the **NTP Servers** field. By default, this new server is enabled, v4 is selected, and the **Prefer No** radio button is selected. If you wish to prefer this server over other servers, click the **Prefer Yes** radio button, and click **Apply**.

- 7. To delete a server, click the corresponding Off radio button, and click Apply.**

Expected outcome

The new server's IP address will disappear from the **NTP Servers** field.

- 8. If you wish to configure a new peer*

Then

Enter the new peer's IP address in the Add New Peer: Address: edit box, and click Apply.

Note

Use IPv6 address(es) and NTP version defaults to v4.

Expected outcome

The new peer's IP address will now appear in the **NTP Peers** field. By default, this new peer is enabled, v4 is selected, and the **Prefer No** radio button is selected. As you add other peers, you may prefer them over the initial peer you configured.

- 9. To add another new peer, repeat step 8.**

Expected outcome

The new peer's IP address will appear in the **NTP Peers** field. By default, this new peer is enabled, v4 is selected, and the **Prefer No** radio button is selected. If you wish to prefer this peer over other peers, click the **Prefer Yes** radio button, and click **Apply**.

- 10. To delete a peer, click the corresponding Off radio button, and click Apply.**

Expected outcome

The new peer's IP address will disappear from the **NTP Peers** field.

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

Further information

See *Network time protocol*