

Nokia High Availability Design and Implementation Documentation

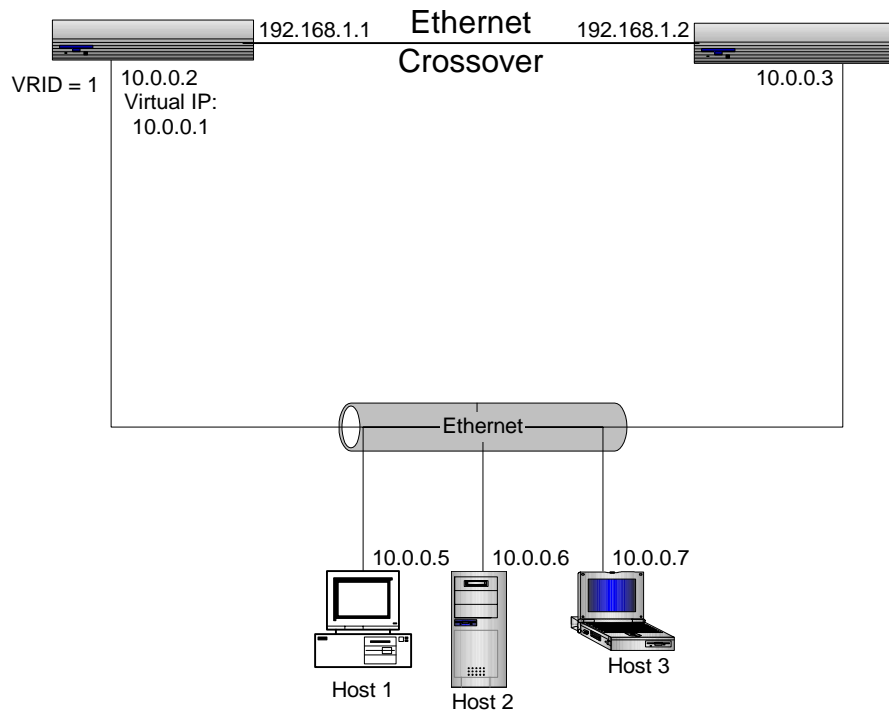
Created By:
Thomas Whang
02/28/00

High Availability Firewall Solution

It was decided that Nokia IP 650s would be the product of choice for redundant infrastructure firewall implementations while the IP 330s would be the product of choice for dedicated customer's redundant firewall implementations. Each firewall pair will have VRRP and state table synchronization active to provide a robust redundant solution.

Solution Overview

High Availability will be provided by VRRP Monitored Circuit and firewall state table synchronization. The following diagram shows a sample network using two Nokias implementing one Virtual Router to back up a single default gateway.



The following figure shows a simple network with two routers implementing one Virtual Router, to back up a single default router. 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 (10.0.0.1) and both Nokias run VRRP.

The Nokia on the left has its address configured as Virtual Router #1 (VRID=1) and the Nokia on the right is the backup for Virtual Router #1. If the Nokia on the left should fail, the other Nokia will take over Virtual Router #1 and its IP addresses and provide uninterrupted service for the hosts. After the Nokia on the left returns to operational state, it will assume all responsibility of Virtual Router #1.

To provide firewall state synchronization and sync time, a private "sync" network is used. This network uses an Ethernet Cat. 5 cross-over cable between both Nokias. This link will be configured for 100Mb Full-Duplex mode.

This document will provide a step by step guide to installing and configuring the IP 650s and IP 330s for the Universal Server Farms.

System Hardware Installation

Nokia IP 650

Installing a New Network Interface Card

You can install a new network interface card (NIC) without powering down the unit.

1. Use a screwdriver to remove the retaining screws holding the blank panel in place.
2. Remove the blank panel.
3. Insert the new NIC. Push it gently into place. Take care to make sure that the card edge is completely seated into the connector inside the unit. If the NIC has an ejector, you can use it to assist in the final seating of the card.
4. Using the screwdriver, screw the retaining screws into place.
5. The unit detects the card. Use Voyager to configure and activate the logical and physical interfaces on the NIC.

Removing a Network Interface Card

You can remove a network interface card (NIC) without powering down the unit.

1. Use Voyager to do the following.
 - A. Deactivate all of the logical interfaces on the NIC.
 - B. Deactivate all of the physical interfaces on the NIC.

If you do not do this before you remove the NIC, you may have to reinstall the NIC before you can deactivate the logical and physical interfaces.

2. Use a screwdriver to remove the retaining screws holding the NIC.
3. Gently pull the NIC forward from the card slot. If the NIC has an ejector, use it to assist you in removing the NIC from the slot.
4. Cover the empty slot with a blank panel and, using a screwdriver, screw the retaining screws into place.

Replacing a Network Interface Card

You can replace a network interface card (NIC) two ways.

- Replace the NIC with a different type (for example, replace an Ethernet NIC with a T1 NIC).
- Replace the NIC with a similar type (for example, replace an Ethernet NIC with another Ethernet NIC). The two NICs do not need to be made by the same manufacturer. They only need to contain interfaces of the same type.

You can perform either replacement without powering down the unit. If you are replacing the NIC in a given slot with a NIC of a similar type, skip to step 2.

1. If you are replacing the NIC with a different type, use Voyager to do the following before you remove the old NIC.
 - A. Deactivate all of the logical interfaces on the NIC.
 - B. Deactivate all the physical interfaces on the NIC.

If you do not do this before you remove the NIC, you may have to reinstall the NIC before you can deactivate the logical and physical interfaces.

2. Use a screwdriver to remove the retaining screws holding the NIC.
3. Gently pull the NIC forward from the card slot. If the NIC has an ejector, use it to assist you in removing the NIC from the slot.

4. Insert the new card. Push it gently into place. Take care to make sure that the card edge is completely seated into the connector inside the unit. If the card has an ejector, you can use it to assist in the final seating of the card.
5. Using a screwdriver, screw the retaining screws into place. The unit detects the card.
6. If you have replaced the NIC with one of a different type, use Voyager to configure and activate the logical and physical interfaces on the NIC.

Replacing a Hard Disk Drive Card

To replace a hard disk drive you *must* power down the unit.

NOTE: If you do not power it down, no harm is done to the unit or the disk drive card, but the operating system will not operate correctly after the card is replaced.

NOTE: Install only one hard disk drive in an IP600 Series unit.

NOTE: Before you can replace a hard disk drive card, you must load it with the appropriate software.

1. Use a screwdriver to remove the retaining screw holding the hard disk drive card.
2. Gently pull the hard disk drive card forward from the card slot. If it has an ejector, use it to assist you in removing the card from the slot.
3. Insert the new hard disk drive card. Push it gently into place. Take care to make sure that the card edge is completely seated into the connector inside the unit. If the card has an ejector, you can use it to assist in the final seating of the card.
4. Using a screwdriver, screw the retaining screw into place.
5. Power up the unit.

Replacing the Fan Drawer

You can change the fan drawer without powering down the unit.

1. Unscrew the screws holding the fan drawer to the chassis.
2. Pull the fan drawer forward to remove it from the chassis.
3. Slide the new fan drawer into the chassis.
4. Screw in the retaining screws with a screwdriver.

WARNING: Do not allow the fan drawer to remain out of the chassis for any longer than is necessary. Components inside the chassis can overheat if they are not cooled for even short periods of time.

Replacing the Power Supply

If the unit contains two power supplies, you can replace one of the power supplies without powering down the unit. Access the power supply from the back of the unit. To remove the power supply, follow these steps.

1. Deactivate the power supply you are replacing by turning the switch off on the back of the power supply.
2. Unplug the power cord from the power supply. All the fans in the power supply should now be turned off.
3. Use a screwdriver to unscrew the two screws that hold the power supply to the chassis.
4. Grasp the handle and pull the power supply toward you. It may require a little extra effort to pull the power supply free from the internal connector.
5. Slide the new power supply into place.
6. Replace the retaining screws and, using a screwdriver, screw them into place.
7. Reconnect the power cord.
8. Turn on the power supply switch.

Nokia IP 330

Installing a New Network Interface Card

To replace a Network Interface Card, you *must* power down the unit.

1. Use a screwdriver to remove the retaining screws holding the blank panel in place.
2. Remove the blank panel.
3. Insert the new NIC. Push it gently into place. Take care to make sure that the card edge is completely seated into the connector inside the unit. If the NIC has an ejector, you can use it to assist in the final seating of the card.
4. Using the screwdriver, screw the retaining screws into place.
5. The unit detects the card. Use Voyager to configure and activate the logical and physical interfaces on the NIC.

System Hardware Configuration

Nokia IP 650 Configuration

The infrastructure Nokia IP 650 will have the following hardware configuration:

- 256 MB RAM
- 5 Quad Fast Ethernet Cards
- 4.5 GB HDD
- 2 Power Supplies

Nokia IP 330 Configuration

The dedicated customer Nokia IP 330 will have the following hardware configuration:

- 128 MB RAM
- 3 Fast Ethernet Ports
- 4.5 GB HDD

System Software Installation

Nokia IP 650 and 330 Installation

The Nokia Network Appliances do not have a CD-ROM or a floppy drive to install the Operating System. All system installs and upgrades will have to be done via the network. To install/upgrade the Operating System, an FTP server with all the files must exist. The following files need to be available to the Nokia:

- ipso.tgz (Operating System)
- f-secure-ssh.tgz (F-Secure SSH Client and Server)
- fw40.SP-4-strong.tgz (Checkpoint FireWall-1 SP4)
- nk-doc32.tgz (Nokia's external/on-line documentation)
- nkflash.bin (Nokia's boot Manager flash)

To install the Nokia Operating System (IPSO 3.2), follow the steps below.

Updating the Boot Manager

You must install an updated Boot Manager *before* installing the IPSO operating system image. To do that, you need a console connection to your NAP. Please follow these steps:

NOTE: Responses that you must type are in **bold** print. IPSO-displayed information is shown in Courier type.

1. Re-mount the root file system in the write mode using the command:
nokia[admin]# mount -uw /
2. Copy nkflash.bin to the /etc directory using the command:
nokia[admin]# cp nkflash.bin /etc
3. Reboot the Nokia using the following command:
nokia[admin]# reboot

The Nokia reboots and displays the following boot prompts:

NOTE: The choices that display for the IP300 and IP 600 series Nokias vary and are shown separately below.

The boot choices for an **IP600 series Nokia** displayed by the Boot Manager are:

```
Rebooting...
Starting bootmgr
Loading boot manager..Bootmgr loaded.Entering
autoboot mode.
Type any character to enter command mode.
Press a key to interrupt the boot process.
BOOTMGR[0]> boot -s
Booting wd(0,f)/image/IPSO-3.2-fcs4-08.17.1999-
124427-783/kernel @ 0xf0100000
.
.
.
Nov 25 06:57:23 init: /etc/spwd.db: No such file or
directory
Enter pathname of shell or RETURN for sh:<Return>
```

The boot choices for an **IP300 series Nokia** displayed by the Boot Manager are:

```
Verifying DMI Pool Data ...
1 . . . Bootmgr
```

```
2 . . . IPSO
Default: 2
```

4. Press the 2 key to boot the IPSO operating system.

```
>> IPSO boot
Usage: [[wd(0,f)]/image/current/kernel] [-abcCdhrsv]
Boot: -s
```

5. At this prompt, enter **-s** and press Enter to boot into the single-user mode:

If you choose to enter number 1 when the `Default: 2` is displayed above in step 4, you see this displayed path:

```
Default: 2
Starting bootmgr
Loading boot manager . . BOOTMGR[0]> boot -s
```

6. Enter **boot -s** at this prompt to boot into the single-user mode. The Nokia reboots into the single-user mode. Now execute the appropriate command for the Nokia for which you want to upgrade the Boot Manager.

7. For an **IP600 series Nokia**, enter:
`/etc/upgrade_bootmgr wd1 /etc/nkflash.bin`
8. For an **IP300 series Nokia**, enter:
`/etc/upgrade_bootmgr wd1 /etc/nkflash.bin`

Full Installation

Place the new IPSO image and any packages you wish to install on an FTP server that is reachable by the machine you are loading.

To do a full installation using downloaded software:

1. Identify the following IP addresses:
 - a. FTP server that contains system software compressed tarfile
 - b. Address of the client (the machine to be installed)
 - c. Address of the default gateway, if any
2. Attach a dumb terminal (a vt100) or terminal emulator to the console serial port (COM1).
3. Power up the Nokia IP650.

The Nokia reboots and displays the following boot prompts:

```
Rebooting...
Starting bootmgr
Loading boot manager..Bootmgr loaded.Entering
autoboot mode.
Type any character to enter command mode.
```

4. Press a key to interrupt the boot process and the Nokia will display the following prompt:

```
BOOTMGR[0]>
```

Start the full IPSO installation by typing the following command:

install

You will see some kernel startup messages, then a dialogue will be presented. The text below displays what you will see and need to type. You will need to substitute your own values for many of the entries. Typed response areas are in bold print. If any entry is not indicated, the default is accepted by selecting Enter.

```
##### IPSO Full Installation #####
You will need to supply the following information:
    Client IP address/netmask, FTP server IP address and filename,
    system serial number, and other license information.
This process will DESTROY any extant files and data on your disk.
#####
```

Continue? (y/n) [n] **y**

Motherboard serial number is IUJN92003476.

The chassis serial number can be found on a sticker on the back of the unit with the letters S/N in front of the serial number.

Please enter the serial number: **8A992507973**

Please answer the following licensing questions.

Please choose a product from the following:

1. IP400 Series
2. IP600 Series
3. IP300 Series

Which product are you installing? :[1]2

Will this node be using IGRP ? [y] **n**

Will this node be using BGP ? [y] **n**

1. Install from anonymous FTP server.
2. Install from FTP server with user and password.

Choose an installation method (1-2): **2**

Enter IP address of this client (0.0.0.0/24): **32.82.30.155**

Please enter a netmask length: (24) **24**

Enter IP address of FTP server (0.0.0.0): **32.82.30.253**

Enter IP address of the default gateway (0.0.0.0): **32.82.30.253**

Choose an interface from the following list:

- 1) eth-slp1
- 2) eth-slp2
- 3) eth-slp3
- 4) eth-slp4
- 5) eth-s2p1
- 6) eth-s2p2
- 7) eth-s2p3
- 8) eth-s2p4

Enter a number [1-8]: **1**

Would you like to use 100 Mb speed for eth-slp1? [n] **y**

Half or full duplex? [h/f] [h] **f**

Enter user name: **nokia**

Enter password for "nokia":

Enter path to ipso.tgz on FTP server [~]: **ipso_3.2**

1. Retrieve all valid packages, with no further prompting.
2. Retrieve packages one-by-one, prompting for each.
3. Retrieve no packages.

Enter choice [1-3] [1]: **1**

Client IP address = 32.82.30.155/24

Server IP address = 32.82.30.253

Default gateway IP address = 32.82.30.253

Network Interface = eth-slp1, speed = 100M, full-duplex

Server download path = [ipso_3.2/]

Package install type = all

Are these values correct? [y] **y**

netlog:eth-slp1 .. enabling 100baseTX/UTP port in half duplex mode

netlog:eth-slp1 .. enabling 100baseTX/UTP port in full duplex mode

Checking what packages are available on 32.82.30.253.

Hash mark printing on (1048576 bytes/hash mark).

Interactive mode off.

#

The following packages are available:

f-secure-ssh.tgz fw40.SP-4-strong.tgz ipso.tgz nk-doc32.tgz

Building filesystems...done.

Making initial links...done.

Downloading compressed tarfile(s) from 32.82.30.253.

Hash mark printing on (1048576 bytes/hash mark).

Interactive mode off.

#

#####

```
#####
#####
#
Checking validity of image...(no system signature file found, continuing)...done.
Checking validity of pkgs...done.
Installing image...done.
Image version tag: IPSO-3.2-fcs4-08.17.1999-124427-783.
Packages being stored in /mnt/opt/tmp .
You will be given a chance to install and activate each package
at your first reboot.
```

Installation completed.

Reset system or hit <Enter> to reboot.

Once rebooted, the Nokia will a variety of reboot and package installation questions.

Starting reboot...

syncing disks... done
Rebooting...

.
.
.
.

No active file. File generation disabled.

Please choose the host name for this system. This name will be used
in messages and usually corresponds with one of the network hostnames
for the system. Note that only letters, numbers, dashes, and dots (.)
are permitted in a hostname.

Hostname? **labnok02**

Hostname set to "labnok02", OK? [y] **y**

Please enter password for user admin:
Please re-enter password for confirmation:

You can configure your system in two ways:

- 1) configure an interface and use our Web-based Voyager via a remote browser
- 2) VT100-based Lynx browser

Please enter a choice [1-2, q]: **1**

Select an interface from the following for configuration:

- 1) eth-slp1
- 2) eth-slp2
- 3) eth-slp3
- 4) eth-slp4
- 5) eth-s2p1
- 6) eth-s2p2
- 7) eth-s2p3
- 8) eth-s2p4
- 9) quit this menu

Enter choice [1-9]: **1**

Enter the IP address to be used for eth-slp1: **32.82.30.155**

Enter the masklength: **24**

Do you wish to set the default route [y] ? **y**

Enter the default router to use with eth-slp1: **32.82.30.253**

This interface is configured as 10 mbs by default.

Do you wish to configure this interface for 100 mbs [n] ? **y**

You have entered the following parameters for the eth-slp1 interface:

```
IP address: 32.82.30.155
masklength: 24
Default route: 32.82.30.253
Speed: 100M
```

You may now configure your interfaces with the Web-based Voyager by typing in the IP address "32.82.30.155" at a remote browser.

```
Generating config files for labnok02 :ipsrd hosts password resolver snmp inetd ttys tz ntp
ssmtp skey arp aggrclass acl syslog aut
osupport httpd done.
```

Sat Feb 26 03:37:04 GMT 2000

```
Loading Packages netlog:eth-slp1 .. enabling 100baseTX/UTP port in half duplex mode
Feb 26 03:37:17 [LOG_INFO] kernel: netlog:eth-slp1 .. enabling 100baseTX/UTP port in half
duplex mode
.. done
```

```
Found packages:
f-secure-ssh.tgz
fw40.SP-3-strong.tgz
fw40.SP-4-strong.tgz
nk-doc32.tgz
```

Package Description: F-Secure SSH client and server, version 1.3.6

Would you like to :

1. Install this as a new package
2. Skip this package

Choose (1-2): 1

```
Installing f-secure-ssh.tgz
Extracting Package
Done installing f-secure-ssh
```

Package Description: Check Point FireWall-1 (Strong) v4.0 SP-4 (Fri Aug 27 09:33:48 PDT 1999 Build 2b)

Would you like to :

1. Install this as a new package
2. Upgrade from an old package
3. Skip this package

Choose (1-3): 1

```
Installing fw40.SP-4-strong.tgz
Extracting Package
Done installing FireWall-1-strong.v4.0.SP-4
```

Package Description: External Documentation for Nokia IPSO 3.2

Would you like to :

1. Install this as a new package
2. Skip this package

Choose (1-2): 1

```
Installing nk-doc32.tgz
Extracting Package
Done installing nokia-doc3.2
cleaning up ..done
System will now reboot to activate packages
```

When the system is rebooted, IPSO 3.2 will be completely installed with all packages installed and active.

Upgrade Installation

To update the Nokia to the IPSO 3.2.1 and later software, use the following procedure.

NOTE: Updating the operating system assumes that a new Boot Manager for IPSO 3.2.1 and greater was successfully downloaded and updated, as described in Updating the Boot Manager.

1. To install the image, enter:

```
newimage -k -R -l filespec
```

Use the -k option to keep all the previously installed packages in their current states. If a package from a previous version of IPSO was enabled and configured to start at boot, it will continue to do so. (The default is for all packages to be disabled by the `newimage` command.) The -R option sets the newly installed IPSO image as the image to use for the next reboot of the platform; the -l option specifies the location of the ipso.tgz file.

2. Type the following at the command-line prompt:

```
nokia[admin]# newimage -k -R -l /var/admin/  
ipso.tgz Validating image...done.  
Version tag stored in image: IPSO-3.2.1-FCS1-  
releng 849 11.24.1999-102644  
Installing new image...done
```

5. Reboot the Nokia.

When the system is rebooted, IPSO 3.2.1 will be completely installed with all packages installed and active.

Installing New Packages

1. Click **CONFIG** on the home page.
2. Click the *Manage Installed Packages* link in the *System Configuration* section.
3. Click the *FTP Packages* link.
4. Enter the FTP site in the **FTP SITE** edit box, the FTP directory in the **FTP DIR** edit box, then click **APPLY**.

NOTE: The new package will appear in the **UNPACK NEW PACKAGES** box.

5. Click on the package you want to install in the **UNPACK NEW PACKAGES** box, then click **APPLY**.
6. To make your changes permanent, click **SAVE**.

System Software Configuration

Nokia IP 650 and 330 Configuration

Ethernet Interfaces

Configuring an Ethernet Interface

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.
Example—
eth-s2p1
4. Click the **10 MBIT/SEC** or the **100 MBIT/SEC** radio button in the **PHYSICAL CONFIGURATION** table **LINK SPEED** field to select the link speed.
5. Click the **FULL** or **HALF** radio button in the **PHYSICAL CONFIGURATION** table **DUPLEX** field to select the duplex mode, then click **APPLY**.
6. Click the logical interface name in the **INTERFACE** column of the **LOGICAL INTERFACES** table to go to the *Interface* page.
7. Enter the IP address for the device in the **NEW IP ADDRESS** edit box.
8. Enter the IP subnet mask length in the **NEW MASK LENGTH** edit box, then click **APPLY**. Each time you click **APPLY**, the configured IP address and mask length are added to the table. The entry fields remain blank to allow you to add more IP addresses.

To enter another IP address and IP subnet mask length, repeat steps 7-8.

9. (Optional) Change the interface's logical name to a more meaningful one by typing the preferred name in the **LOGICAL NAME** edit box, then click **APPLY**.
10. Click the **UP** button to go to the *Interface Configuration* page.
11. Click the **ON** radio button that corresponds to the logical interface you have configured, then click **APPLY**. The Ethernet interface is now available for IP traffic and routing.
12. To make your changes permanent, click **SAVE**.

Changing the Speed of an Ethernet Interface

If the link speed of an Ethernet interface is incorrect, it will not send or receive data. The following steps describe how to change the speed of an Ethernet interface.

1. Click **CONFIG** on the home page.
2. Click the *Interfaces* link.
3. Click the physical interface link you want to change in the **PHYSICAL** column.
Example—
eth-s2p1
4. Click the **10 MBIT/SEC** or the **100 MBIT/SEC** radio button in the **PHYSICAL CONFIGURATION** table **LINK SPEED** field, then click **APPLY**.
5. To make your changes permanent, click **SAVE**.

Changing the Duplex of an Ethernet Interface

If the link speed of an Ethernet interface is incorrect, it will not send or receive data. The following steps describe how to change the speed of an Ethernet interface.

6. Click **CONFIG** on the home page.
7. Click the *Interfaces* link.
8. Click the physical interface link you want to change in the **PHYSICAL** column.
Example—
eth-s2p1

9. Click the **FULL** or **HALF** radio button in the **PHYSICAL CONFIGURATION** table **DUPLEX** field, then click **APPLY**.
10. To make your changes permanent, click **SAVE**.

Changing the IP Address of an Ethernet Interface

NOTE: Do not change the IP address you use in your browser to access Voyager. If you do, you can no longer access the unit with your browser.

1. Click **CONFIG** on the home page.
2. Click the *Interfaces* link.
3. Click the logical interface link for which you want to change the IP address in the **LOGICAL** column.
Example—
eth-s2p1c0
4. To remove the old IP address, click the **DELETE** check box that corresponds to the address you want to delete, then click **APPLY**.
5. To add the new IP address, enter the IP address for the device in the **NEW IP ADDRESS** edit box.
6. Enter the IP subnet mask length in the **NEW MASK LENGTH** edit box, then click **APPLY**.
Each time you click **APPLY**, the newly configured IP address and mask length are added to the table. The entry fields remain blank to allow you to add more IP addresses.
7. To make your changes permanent, click **SAVE**.

Hostname

Changing Hostname

1. Click **CONFIG** on the home page.
2. Click the *Change Hostname* link in the *System Configuration* section.
3. Enter the new hostname in the **CHANGE IT TO** field, then click **APPLY**.
4. To make your changes permanent, click **SAVE**.

Adding a Static Host

1. Click **CONFIG** on the home page.
2. Click the *Host Address Assignment* link in the *System Configuration* section.
3. Enter the new hostname in the **ADD NEW HOSTNAME** edit box, then click **APPLY**.
4. Enter the IP address of the new host in the **IP ADDRESS** edit box, then click **APPLY**.
5. To make your changes permanent, click **SAVE**.

Removing a Static Host

1. Click **CONFIG** on the home page.
2. Click the *Host Address Assignment* link in the *System Configuration* section.
3. Click the **OFF** radio button next to the host you want to delete, then click **APPLY**.
4. To make your changes permanent, click **SAVE**.

Configuring Static Routes

Creating a Default Route

1. Click **CONFIG** on the home page.
2. Click the *Static Routes* link in the *Routing Configuration* section.
3. Click the **ON** radio button in the **DEFAULT STATIC ROUTE** field, then click **APPLY**.
4. Enter the IP address of the default router in the **ADDITIONAL GATEWAY** edit box, then click **APPLY**.
5. To make your changes permanent, click **SAVE**.

Disabling a Default Route

1. Click **CONFIG** on the home page.
2. Click the *Static Routes* link in the *Routing Configuration* section.
3. Click the **OFF** radio button in the **DEFAULT STATIC ROUTE** field, then click **APPLY**.
4. To make your changes permanent, click **SAVE**.

Creating a Static Route

1. Click **CONFIG** on the home page.
2. Click the *Static Routes* link in the *Routing Configuration* section.
3. Enter the network prefix in the **NEW STATIC ROUTE** edit box.
4. Enter the mask length (number of bits) in the **MASK LENGTH** edit box, then click **APPLY**.
5. Enter the IP address of the next hop router in the **GATEWAY** edit box, then click **APPLY**.
6. To make your changes permanent, click **SAVE**.

SNMP

Enabling SNMP Monitoring

1. Click **CONFIG** on the home page.
2. Click the *SNMP* link.
3. (Optional) If you want to change the read-only community string, enter the name in the **CHANGE READ-ONLY COMMUNITY STRING** edit box, then click **APPLY**.
4. (Optional) Enter an SNMP location string in the **SNMP LOCATION STRING** edit box, then click **APPLY**.
5. (Optional) Enter an SNMP contact string in the **SNMP CONTACT STRING** edit box, then click **APPLY**.
6. To make your changes permanent, click **SAVE**.

Sending SNMP Traps

1. Click **CONFIG** on the home page.
2. Click the *SNMP* link.
3. Enter the IP address of a new receiver that will accept traps from this device in the **ADD NEW RECEIVER** edit box, then click **APPLY**.
4. Enter the community string for the specified receiver in the **COMMUNITY** edit box.

NOTE: Link state and cold start traps are always enabled and cannot be disabled.

5. (Optional) If you want to enable authentication traps, click the **ON** radio button next to the **ENABLE AUTHENTICATION TRAPS** field, then click **APPLY**.
6. To make your changes permanent, click **SAVE**.

Time and Date

Setting the System Time

1. Click **CONFIG** on the home page.
2. Click the *Local Time Setup* link in the *System Configuration* section.
3. Click the appropriate time zone in the **TIME ZONE** drop-down list.
4. Enter the hour in the **HOUR** edit box, the minute(s) in the **MINUTE** edit box, the second(s) in the **SECOND** edit box, the month in the **MONTH** edit box, the day in the **DAY** edit box, and the year in the **YEAR** edit box, then click **APPLY**.
5. To make your changes permanent, click **SAVE**.

NOTE: If there is no NTP server, the primary Nokia must be the NTP server and must have its system time configured.

NTP

Primary Nokia

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, then click **APPLY**.
The NTP configuration page will display.

4. Enter the new server's IP address in the **ADD NEW SERVER: ADDRESS:** edit box, then click **APPLY**. The new server's IP address will now appear in the **NTP SERVERS** field. To make your changes permanent, click **SAVE**.

NOTE: The NTP server's IP address will be the primary Nokia's crossover link IP address.

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

Secondary Nokia

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, then click **APPLY**.
The NTP configuration page will display.
4. Enter the new server's IP address in the **ADD NEW SERVER: ADDRESS:** edit box, then click **APPLY**. The new server's IP address will now appear in the **NTP SERVERS** field.

NOTE: The NTP server's IP address will be the primary Nokia's crossover link IP address.

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

VRRP

Description

Virtual Redundant Router 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 blackhole 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.

Creating a Virtual Router in Monitored Circuit Mode

1. Click **CONFIG** on the home page.
2. Click the **VRRP** link in the *Router Services* section.
3. Click the **MONITORED CIRCUIT** radio button, then click **APPLY**.
4. Enter the VRID (numeric value between 1 and 255) in the **CREATE VIRTUAL ROUTER** edit box, then click **APPLY**.
5. Enter the IP address (Virtual IP address) of the router you want to have the virtual router back up in the **BACKUP ADDRESS** edit box, then click **APPLY**.

NOTE: The IP address is the address of the default router that all hosts will point to. It must be in the same IP subnet as one of the addresses on this interface.

6. Repeat this step if you want to add additional IP addresses.
7. (Optional) Enter a number in the **PRIORITY** edit box, then 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, then click **APPLY**.
9. Select the interface that you want to monitor from the **MONITOR INTERFACE** drop-down window, then click **APPLY**.
10. Enter a number in the **PRIORITY DELTA** edit box, then 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

11. (Optional) Repeat steps 8 and 9 if you want to add more monitored interface dependencies.
12. To make your changes permanent, click **SAVE**.

Removing a Virtual Router in Monitored Circuit Mode

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, then 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**.

Changing the Priority of a Virtual Router in Monitored Circuit Mode

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

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, then 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**.

Changing the Hello Interval of a Virtual Router in Monitored Circuit Mode

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, then 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**.

Changing the IP Address List of a Virtual Router in Monitored Circuit Mode

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.

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, then click **APPLY**.

- To add an IP address to the list, enter the IP address in the **BACKUP ADDRESS** edit box, then click **APPLY**.

NOTE: The IP address is the address of the default router that all hosts will point to. It must be in the same IP subnet as one of the addresses on this interface.

- To make your changes permanent, click **SAVE**.

Changing the List of Monitored Interfaces in Monitored Circuit Mode

- Click **CONFIG** on the home page.
- Click the **VRRP** link in the *Router Services* section.
- Select the interface that you want to monitor from the **MONITOR INTERFACE** drop-down window, then click **APPLY**.
- Enter a number in the **PRIORITY DELTA** edit box, then 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

- To remove an interface from being monitored, click the corresponding **OFF** radio button, then click **APPLY**.
- To change the priority delta, enter a new number in the **PRIORITY DELTA** edit box, then click **APPLY**.
- To make your changes permanent, click **SAVE**.

Changing Authentication Method and Password in Monitored Circuit Mode

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.

- Click **CONFIG** on the home page.
- Click the **VRRP** link in the *Router Services* section.
- Locate the interface with the authentication method or password you want to change.
- Click the **NONE** or **SIMPLE** radio button to select the authentication method used by VRRP on this interface's LAN, then click **APPLY**. The value in this field must be the same for all routers running VRRP on this interface's LAN.
- If you selected **SIMPLE**, enter the authentication password string in the **PASSWORD** edit box, then click **APPLY**. The value in this field must be the same for all routers running VRRP on this interface's LAN.
- To make your changes permanent, click **SAVE**.

The following is a sample configuration of VRRP Monitored Circuit:

Primary:

```
eth-s1p2c0 32.97.167.248/24
Authentication:    None
Virtual Router:    167
Priority:           110
Priority Delta:     20
Hello Interval:    25
Backup IP:         32.97.167.250
Monitor Interfaces: eth-s1p3c0,eth-s1p4c0
```

```
eth-s1p3c0 32.97.169.2/24
Authentication:    None
Virtual Router:    169
Priority:           110
Priority Delta:     20
Interval:          5
```

Secondary:

```
eth-s1p2c0 32.97.167.249/24
Authentication:    None
Virtual Router:    167
Priority:           100
Priority Delta:     20
Hello Interval:    25
Backup IP:         32.97.167.250
Monitor Interfaces: eth-s1p3c0,eth-s1p4c0
```

```
eth-s1p3c0 32.97.169.3/24
Authentication:    None
Virtual Router:    169
Priority:           100
Priority Delta:     20
Hello Interval:    5
Hello
```

Backup IP:	32.97.169.1	Backup IP:	32.97.169.1
Monitor Interfaces:	eth-s1p4c0, eth-s1p2c0	Monitor Interfaces:	eth-s1p4c0, eth-s1p2c0
eth-s1p4c0 32.97.170.2/24		eth-s1p4c0 32.97.170.3/24	
Authentication:	None	Authentication:	None
Virtual Router:	170	Virtual Router:	170
Priority:	110	Priority:	100
Priority Delta:	20	Priority Delta:	20
Hello Interval:	5	Hello Interval:	5
Backup IP:	32.97.170.1	Backup IP:	32.97.170.1
Monitor Interfaces:	eth-s1p2c0, eth-s1p3c0	Monitor Interfaces:	eth-s1p2c0, eth-s1p3c0

The above configuration has three VRRP instances. (VRID 167, 169, 170) Each VRRP Backup Address (32.97.167.250, 32.97.169.1, 32.97.170.1) is the default gateway for all hosts in their respective subnets.

Configuring the Firewall with VRRP Monitored Circuit

The following assumption is made regarding the configuration of the firewall:

- Firewall synchronization is already configured and working.
- Firewall is running with an existing rulebase.

The firewall needs to be configured to allow VRRP traffic.

1. Create new **Workstation** firewall objects with the IP addresses of the Nokia interfaces.
2. Define new **Other** service with the following parameters:
 - Name: VRRP
 - Match: ip_p = 0x70
3. Create new **Workstation** firewall object with the IP address of 224.0.0.18. (VRRP Multicast Address)
4. Add the following rule to allow VRRP traffic through the firewall.
 - Source: All interfaces of both Nokias except the sync interface.
 - Destination: VRRP Multicast Address (224.0.0.18)
 - Service: VRRP
 - Action: Accept
5. Add the following rule to the firewall to allow both firewall sync firewall state tables and sync time using NTP.
 - Source: Sync interfaces of both Nokias.
 - Destination: Sync interfaces of both Nokias.
 - Service: FireWall, NTP
 - Action: Accept

The following is a sample configuration of the firewall:

Workstation Objects:

- H_192.168.20.1 (Primary Nokia Sync IP)
- H_192.168.20.2 (Secondary Nokia Sync IP)
- H_32.97.167.248 (Primary Nokia 167 IP)
- H_32.97.169.2 (Primary Nokia 169 IP)
- H_32.97.170.2 (Primary Nokia 170 IP)
- H_192.168.20.2 (Secondary Nokia Sync IP)
- H_32.97.167.249 (Secondary Nokia 167 IP)
- H_32.97.169.3 (Secondary Nokia 169 IP)
- H_32.97.170.3 (Secondary Nokia 170 IP)
- H_224.0.0.18 (VRRP multicast address)

VRRP Service object:

- Name: VRRP
- Match: ip_p = 0x70

Firewall Rules:

- Source: H_192.168.20.1, H_192.168.20.2
- Destination: H_192.168.20.1, H_192.168.20.2
- Service: FireWall1, NTP
- Action: Accept

- Source: H_32.97.167.248, H_32.97.169.2, H_32.97.170.2, H_32.97.167.249, H_32.97.169.3, H_32.97.170.3
- Destination: N_224.0.0.18
- Action: Accept

Managing Packages

Enabling Packages

1. Click **CONFIG** on the home page.
2. Click the *Manage Installed Packages* link in the *System Configuration* section.
3. Click the **ON** radio button in front of the package you want to enable, then click **APPLY**.
4. Click **SAVE**.

NOTE: To activate the new package, you must reboot the system as follows:

5. Click **TOP**.
6. Click the *Shut Down System* link.
7. Click the **REBOOT** button. The system will take a few minutes to reboot.

Disabling Packages

1. Click **CONFIG** on the home page.
2. Click the *Manage Installed Packages* link in the *System Configuration* section.
3. Click the **OFF** radio button in front of the package you want to disable, then click **APPLY**.
4. To make your changes permanent, click **SAVE**.

Deleting Packages

1. Click **CONFIG** on the home page.
2. Click the *Manage Installed Packages* link in the *System Configuration* section.
3. Click the *Delete Packages* link.
4. Click the **DELETE** radio button in front of the package you want to delete, then click **APPLY**.
5. To make your changes permanent, click **SAVE**.