IPSO 3.6 FCS 6
Getting Started Guide and Release Notes

Part No. N450930001 Rev A

Published February, 2003

Corporate Headquarters

Email	info@iprg.nokia.com
Web Site	http://www.nokia.com
Telephone	1-888-477-4566 *or* 1-650-625-2000
Fax	1-650-691-2170
Mail Address	Nokia Inc. 313 Fairchild Drive Mountain View, California 94043-2215 USA

Regional Contact Information

Americas	Nokia Inc. 313 Fairchild Drive Mountain View, CA 94043-2215 USA	Tel: 1-877-997-9199 Outside USA and Canada: +1 512-437-7089 e-mail: info.ipnetworking_americas@nokia.com
Europe	Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG U.K	Tel: 00800 5543 1816 or 1+44 (0) 8700 555 777 e-mail: info.ipnetworking_emea@nokia.com
Asia-Pacific		Tel: +358 9 692 7156 e-mail: info.ipnetworking_apac@nokia.com

Nokia Customer Support

Web Site:	https://support.nokia.com/
Email:	tac.support@nokia.com
	Americas
Voice:	1-888-361-5030 or 1-613-271-6721
Fax:	1-613-271-8782
	Europe
Voice:	+44 (0) 125-286-8900
Fax:	+44 (0) 125-286-5666
	Asia-Pacific
Voice:	+65-7232999
Fax:	+65-7232897

010827

Contents

1 New Features in Nokia IPSO 3.6 OS

Nokia is pleased to announce several enhancements to the IPSO operating system used on Nokia appliances.

For more information about IPSO 3.6 FCS 6, log onto the Nokia customer support site at https://support.nokia.com, click on the Knowledge Base link, and access resolution 15686.

What's New in IPSO 3.6 FCS 6

IPSO 3.6 FCS 6 is a full version of the IPSO operating system and contains the following enhancements to the previous releases of IPSO 3.6:

- SNMP traps fixed
- Fault manager disabled
- Fixes for occasional hangs and crashes
- EBGP negotiation issue fixed
- Configuring BGP with loopback address
- Improved small packet throughput
- Hot swapping disks into IP700 appliances improved
- OSPF sending unnecessary LSAs fixed
- RealSecure memory leak fixed

- PIM issue fixed
- Vulnerability fixed
- Message displayed after automatic reboot
- NAT/clustering issue fixed
- IGMP/clustering

SNMP Traps Fixed

Some IPSO system trap OIDs have been changed in the file NOKIA-IPSO-SYSTEM-MIB.txt.

The previous OIDs were

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).
nokia(94).nokiaProducts(1).ipsoProducts(21).
ipsoSystem(1).ipsoNotificationGroup.systemTraps. *specific_trap*

The new OIDs are

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).
nokia(94).nokiaProducts(1).ipsoProducts(21).
ipsoSystem(1).ipsoSystemTrapsPrifix(0). *specific_trap*

Any scripts using the previous OIDs should be updated to reflect this change.

Instructions for HP OpenView Users

If you use HP OpenView, perform the following procedure

1. Unload the existing NOKIA-IPSO-SYSTEM-MIB.
2. Open Event Configuration.
3. Delete the events under ipsoNotificationGroup and the enterprise ipsoNotificationGroup.
4. Save the changes.
5. Load the new MIB.

6. Configure the events to report or log as required.

   Be sure to configure each event that you want to see information for.

VRRP Traps

In previous releases of IPSO 3.6, the snmpTrapOID lacked a 0 in all the VRRP traps. This is corrected in FCS 6.

Fault Manager Disabled

In FCS 6, IPSO's fault management feature is disabled by default. It is disabled to prevent confusion over the traps that are generated by the fault management daemon (fmd) when the feature is enabled.

If you want to use the fault management feature, you must enable it by following these steps:

1. Log into your appliance using Nokia Network Voyager.
2. Click Config.
3. Under Fault Management Configuration, click General Configuration.
4. In the Fault Management field, select Enabled.
5. Click Apply.

Fix for Occasional Hangs and Crashes

Nokia appliances running VPN-1/FireWall-1 and previous versions of IPSO 3.6 can sometimes hang (freeze) or crash and reboot under certain conditions (for example, when there are a large number of connections). FCS 6 contains fixes that minimize these problems.

EBGP Negotiation Issue Fixed

With previous releases of IPSO 3.6, appliances running External Border Gateway Protocol (EBGP) can fail to renegotiate peering after they are rebooted. FCS 6 fixes this problem.

Configuring BGP with Loopback Address

You can now configure BGP on a loopback address (so that if a real BGP interface fails, BGP will remain enabled).

Improved Small Packet Throughput

With previous releases of IPSO 3.6 running VPN-1/FireWall-1, the throughput for smaller packets (64, 128, and 256 bytes) was less than with IPSO 3.5 and VPN-1/FireWall-1. This has been corrected—IPSO 3.6 FCS 6 with VPN-1/FireWall-1 has better throughput for smaller packets than IPSO 3.5 and VPN-1/FireWall-1.

Hot Swapping Disks into IP700 Appliances Improved

Nokia IP700 Series appliances support disk mirroring when running IPSO 3.6. If the boot drive is installed in drive slot A, you can install a disk drive into slot B without turning off the appliance. That is, you can hotswap a drive into slot B.

However, if the system is running a version of IPSO prior to FCS 6 and the drive you hotswap into drive B was previously part of a mirror set *on the same appliance*, the appliance may crash.

This issue is corrected in FCS 6. You can safely hotswap a drive into slot B of an IP700 Series appliance even if the drive was previously part of a mirror set on the same appliance.

OSPF Sending Unnecessary LSAs Fixed

In previous releases of IPSO 3.6, the routing protocol Open Shortest Path First (OSPF) unnecessarily retransmits link state advertisements. This issue is corrected in FCS 6.

RealSecure Memory Leak Fixed

When used with previous releases of IPSO 3.6, RealSecure for Nokia 7.0 leaks a significant amount of memory. This is fixed in FCS 6.

PIM Issue Fixed

When running Protocol-Independent Multicast (PIM) protocol, earlier releases of IPSO 3.6 can incorrectly prevent traffic from being forwarded under a specific condition.

When a source stops sending multicast traffic for a period of time and the corresponding multicast route entry (MRT) expires, IPSO sends a prune upstream before deleting this entry. If the source sends traffic again before the holdtime of the prune message expires on any of the upstream routers, traffic is temporarily suppressed.

This problem is fixed in FCS 6. A corresponding prune is not sent upstream when an inactive MRT entry expires.

Vulnerability Fixed

Previous releases of IPSO 3.6 are vulnerable to the buffer overflow issue discussed in CERT's Vulnerability Note VU#844360. (The note is available at http://www.kb.cert.org/vuls/id/844360.) FCS 6 is not vulnerable to this problem.

Message Displayed After Automatic Reboot

When previous releases of IPSO 3.6 are rebooted automatically because a hang is detected, the system does not display a message indicating what occurred. FCS 6 does display an explanatory message if this happens.

NAT/Clustering Issue Fixed

With previous releases of IPSO 3.6, routing problems can occur if all the following conditions are true:

- an IPSO cluster is connected to two or more internal networks (such as a production network and a DMZ)
- Check Points' VPN-1/FireWall-1 is running on the cluster
- NAT is configured on the cluster

If all these conditions apply, traffic between the internal networks protected by the cluster is subject to routing asymmetries. When asymmetries occur, packets are dropped.

FCS 6 fixes this problem, but you also need to configure VPN-1/FireWall-1 so that the internal networks do not use NAT when communicating with each other. To do so, create NAT rules as shown below.

Original Packet			Translated Packet		
Source	**Destination**	**Service**	**Source**	**Destination**	**Service**
Net_A	Net_B	Any	Original	Original	Original
Net_B	Net_A	Any	Original	Original	Original

Note
Remember that in this example Net_A and Net_B are internal networks.

IGMP/Clustering

If you use IPSO clustering and use a data (production) network as the cluster primary network, IPSO's cluster protocol messages are propagated throughout the network. This is an unproductive use of bandwidth because cluster protocol messages are used only by IPSO cluster nodes.

If you use FCS 6, you can prevent the cluster protocol messages from being spread across the network by connecting the network with a switch that is capable of IGMP snooping.

FCS 6 sends out IGMP membership reports for the cluster protocol multicast group. The switch will then forward cluster protocol messages only to group members—that is, the other cluster nodes. It will not forward the cluster protocol to ports that are not connected to cluster nodes.

IPSO clusters running earlier releases of IPSO 3.6 do not send out IGMP membership reports, which means that connected switches cannot form multicast groups that comprise the cluster nodes. If you use a data network as a cluster primary network with these releases, you cannot prevent cluster protocol traffic from being propagated across the network.

Note
Nokia recommends that you use a dedicated network as the primary cluster network—the primary cluster network should not carry production data traffic. If you configure a cluster this way, the cluster protocol messages will not appear on your data networks even if the switches on the data networks do not support IGMP snooping.

Note
If you run Check Point's VPN-1/FireWall-1 with an IPSO cluster and want to use this configuration (use a data network for cluster protocol traffic but prevent the cluster messages from propagating beyond the cluster), you must use VPN-1/FireWall-1 NG FP3 with hotfix 1 or later.

What's New in IPSO 3.6

IPSO 3.6 contains the following new features and enhancements to existing features:

- Command-line interface
- High-availability firewall clusters
- Disk mirroring
- TACACS+ Client
- Monitoring enhancements
- SNMP enhancements
- Partner applications

Command-Line Interface

You can now use a command-line interface (CLI) to configure and monitor IPSO systems. The CLI complements Nokia Network Voyager, Nokia's web-based interface for IPSO systems, by allowing you to chose the interface you are most comfortable with.

Everything that you can accomplish with Voyager can also be done with the CLI. You can enter CLI commands individually and you can also create "batch files" of CLI commands to automate configuration tasks.

For detailed information about how to use the CLI, see the *CLI Reference Guide for IPSO 3.6*. You can access the *CLI Reference Guide* by clicking the *Doc* button on the Nokia Network Voyager home page and then clicking the link for this document. The document is also available on the Nokia customer support web site.

High-Availability Firewall/VPN Clusters

IPSO 3.6 lets you create firewall/VPN clusters that provide fault tolerance and dynamic load balancing. A cluster is made up of multiple appliances (nodes)

that share a common IP address and multicast MAC address, and it appears as a single system to the networks on either side of it.

A cluster continues to function if a node fails or is taken out of service for maintenance purposes, and there is no single point of failure. IPSO clusters are also scalable with regard to VPN performance—as you add nodes to a cluster you see improvements in VPN throughput.

IPSO firewall clusters support a variety of Check Point VPN-1/FireWall-1 NG features, including:

- Synchronizing state information between firewalls
- Firewall flows
- Network address translation
- VPN encryption

It is easy to create and manage a cluster. IPSO and the firewall/VPN are monitored on each appliance, and each appliance also monitors the state of the cluster.

Clustering is best suited for LAN applications because the cluster nodes must not use dynamic routing.

Supported Appliances

You can implement clusters using the following appliances:

- IP740
- IP710
- IP650
- IP530
- IP440
- IP330

Base your choice of appliances on your objectives for creating the cluster:

- To provide fault tolerance for your firewall or VPN, you can use all these appliances.
- To get the benefits of load balancing firewall traffic, use the IP740.

- To achieve significant VPN performance improvements, use the IP740, IP710, and IP530.

Routers Facing Firewall/VPN Clusters

Because all the nodes of an IPSO cluster share a single multicast MAC address, routers that connect to a cluster (either directly or through a switch or hub) must be able to accept ARP replies that contain a multicast MAC address. To configure a Nokia IPSO appliance to do this, follow these steps:

1. Connect to the appliance using Nokia Network Voyager.
2. On the Voyager home page, click *Interface Configuration*.
3. Click *ARP*.
4. Under Global ARP Settings, click the button to enable the appliance to accept multicast ARP replies.

For information about how to perform this procedure with the CLI, see the *CLI Reference Guide for IPSO 3.6*.

Switch Requirements

Because all the nodes of a cluster share a single multicast MAC address, the network switches that you install on either side of a cluster must be capable of processing these addresses, that is, they must be able to forward packets destined for a single (multicast) MAC address out multiple switch ports. Nokia recommends that you use the following switches for this purpose:

- Cisco Catalyst 6500
- Nortel Networks Passport 8600
- Extreme Networks Blackdiamond
- Extreme Networks Alpine 3804
- Foundry Network BigIron 4000

Disk Mirroring

The Nokia disk mirroring feature provides fault tolerance by letting the IP500 and IP700 Series appliances continue working in the event of a disk failure. You can create mirror sets that consist of a source disk (which holds the active copy of the operating system) and mirror hard disk. The mirror disk contains a copy of all the files on the source disk, and if the source disk fails, the mirror disk immediately takes over. The IP500 or IP700 Series appliance continues to operate normally.

If you have an IP700 Series appliance on which you configured disk mirroring, you can "hot swap" disk drives—you can replace a drive without shutting down the appliance. This allows you to replace a failed drive without interrupting service. (You cannot hot swap disk drives in an IP530.)

You can use Nokia Network Voyager, the CLI, or Lynx to create and delete mirror sets.

TACACS+ Client

IPSO 3.6 supports the Terminal Access Controller Access Control System Plus (TACACS+) protocol (as a client only) for authenticating IPSO logins.

TACACS+ is an authentication mechanism that allows a remote server not running IPSO to authenticate users on behalf of the IPSO system. TACACS+ encrypts transmitted passwords and other data for security.

In IPSO 3.6, TACACS+ is supported for authentication only, not for accounting. Challenge/response authentication (such as S/Key) over TACACS+ is not supported by IPSO.

You can configure TACACS+ separately for various services. When TACACS+ is configured for use with a service, IPSO contacts the TACACS+ server each time it needs to verify a user name and password.

TACACS+ (identified as TACPLUS) is available as an option in the Auth. Profile section of the AAA Configuration page in Nokia Network Voyager. You can also use CLI commands to configure the system to use TACACS+.

Monitoring Enhancements

IPSO 3.6 offers a number of enhanced monitoring capabilities. You can now obtain current and historical reports on CPU and memory utilization, and all the current and historical reports allow you to view the report data in a graphical format as well as a tabular format. You can also view report data in a delimited-text format that is suitable for downloading (and then importing into a tool that allows you to manipulate the data however you like).

The appropriate current and historical reports are improved to allow you more flexibility in choosing the data to view. For example, on the Interface Throughput Report page you can select multiple interfaces for data collection and choose multiple types of throughput to measure.

SNMP Enhancements

NTP MIB

Earlier versions of IPSO did not have an SNMP MIB for the network time protocol (NTP), so NTP control and monitoring functions could not be performed with SNMP tools. NTP provides for the synchronization of networked devices and is vital for the health of the network, so it is important that it is manageable with SNMP. With version 3.6, IPSO provides this capability.

ipCidrRouteTable Supported

IPSO 3.6 supports ipCidrRouteTable, as defined in RFC 2096. ipRouteTable, as defined in RFC 1213, is deprecated.

Multiple ATM Virtual Paths

You can now configure as many as 256 virtual paths per ATM interface. The allowed number of virtual channels per virtual path ranges from 15 to 4095,

depending on the number of possible virtual paths. Table 1 shows the combinations of VPI and VCI ranges.

Table 1 VPI and VCI Ranges

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

Partner Applications

The Nokia IPSO 3.6 operating system supports the following partner applications on Nokia appliances. The features and operation of the available applications are described in separate documents.

- Check Point VPN-1/FireWall-1 Next Generation (NG), Feature Packs 2 and 3
- RealSecure for Nokia, version 6.5 (intrusion detection system)

2 Using DHCP to Configure the System

You can use the built-in dynamic host configuration protocol (DHCP) client to configure your Nokia system instead of using a console (direct serial) connection. This feature allows a properly configured DHCP server to provide your system with a

- Host name
- IP address
- Default route

You can then use Nokia Network Voyager to reconfigure any of these settings. Once do so, Voyager keeps the modified settings. (DHCP is not used if configuration information exists.) The DHCP server automatically sets the administrative password of the IP system to `password`.

Note
If you intend to use a console connection to configure the system, read "If You Use a Console Connection to Configure the System" on page 26 before you proceed.

To use DHCP to configure your system, perform the following steps (which are explained in the following sections):

1. Configure the DHCP server.
2. Run the DHCP client on the Nokia system.

Configure the DHCP Server

Configure a DHCP server with (at a minimum) mappings for

- A host name for the Nokia system
- The serial number of the appliance
- A static IP address for the appliance

(IPSO also supports MAC-address based configuration.)

The minimum IP address lease required is one year.

Note
The DHCP server must be on the same network as the Nokia appliance or DHCP/BOOTP relay must be configured on the intermediate routers.

Below is an example of relevant DHCP configuration information:

```
ddns-update-style ad-hoc;
subnet 10.1.1.0 netmask 255.255.255.0 {

   # default gateway
   option routers                  10.1.1.1;
   option subnet-mask              255.255.255.0;

   option time-offset              -8;
   option domain-name-servers      24.5.207.179;

   range dynamic-bootp 10.1.1.20 10.1.1.100;
   default-lease-time -1;
   max-lease-time -1;

   host IP710fixed {
      # serial number of the box
      option dhcp-client-identifier "123456";

      fixed-address 10.1.1.11;
      option host-name "IP710";
   }
}
```

Running the DHCP Client on the Nokia System

Note
Do not perform the following procedures unless you configured an appropriate DHCP server with configuration information for your appliance.

1. Connect a NIC installed in your appliance to your network.
2. Turn the appliance on.

The DHCP client program in the system starts automatically, and the DHCP server provides the appropriate configuration information. (This can require 5 to 10 minutes.)

3. From a computer on the same network, ping the IP address that you configured the DHCP server to provide to the Nokia system.

   When you get replies from `ping`, you can use Nokia Network Voyager to connect to the system.

4. Connect to the system using Voyager.

   To connect, start a Web browser and enter the IP address or host name of the system in the address or URL field of the browser.

5. Enter the user name `admin` and the password `password`.

6. Modify the configuration of the system as appropriate.

Note
Nokia strongly recommends that you change the password.

If You Use a Console Connection to Configure the System

If you use a console connection to configure the Nokia system, the system prompts you for the appropriate configuration settings the first time you turn it on. The first prompt asks you to supply a host name. If you wait more than approximately 30 seconds before you type a response to the host name prompt, the DHCP client program starts automatically, and the system might be provided a host name and IP address that is unknown to you. (This could happen if a DHCP server on your network is configured to supply configuration information to any system that requests it.)

In this situation, you cannot connect to the Nokia system over the network (because you don't know the system's IP address or host name). To resolve the problem, follow these steps.

1. Establish a console connection to the system.
2. Enter

   ```
   rm /config/active
   ```

   or

   ```
   mv /config/active /config/active.old
   ```
3. Reboot the appliance.
4. Respond to the configuration prompts in a timely manner.

3 Installing IPSO 3.6

You can upgrade directly to IPSO 3.6 from the following IPSO versions:

- 3.3
- 3.3.1
- 3.4
- 3.4.1
- 3.4.2
- 3.5

You can also revert to those earlier versions of IPSO from IPSO 3.6 if you previously installed them on your appliance.

Caution
Do not upgrade IP350 and IP380 appliances to IPSO 3.6. These systems do not work with versions of IPSO other than 3.5.1.

Note
If you use Nokia Horizon Manager to manage your appliances, you can configure it to upgrade and revert to earlier versions of IPSO on your appliances.

You can install IPSO (and packages) using

- Nokia Horizon Manager

- Nokia Network Voyager
- IPSO CLI
- IPSO command shell (console session)

Upgrading From IPSO 3.5

If you intend to upgrade from IPSO 3.5 to IPSO 3.6, read this section before proceeding.

If your version of IPSO 3.5 is FCS 11 or earlier, there are no issues.

If your version of IPSO 3.5 is FCS 12 or later and you upgrade to a version of IPSO 3.6 earlier than FCS 6, the following problems will occur:

- Your configuration information will be lost.
- It will be possible to log into your IPSO system without supplying a password.

To avoid these issues, upgrade to IPSO 3.6 FCS 6 or later.

Where to Get IPSO 3.6

You can obtain IPSO 3.6 from the CD-ROM that is provided with the Nokia IPSO 3.6 Release Pack. You can also obtain IPSO 3.6 by downloading the software from the Nokia support site at https://support.nokia.com.

Downloading IPSO 3.6 From the Support Site

1. Type https://support.nokia.com in the URL field of your browser and press Enter.
2. Log in using your user name and password.
3. Click *Software Downloads*.
4. Click the *IPSO 3.6 Release Notes and Download* link.

5. Before you click this link, copy or take note of the MD5 value.
6. Copy or take note of the MD5 value under the *IPSO 3.6* link under "IPSO Operating System only."
7. Click *IPSO 3.6* link.
8. Download the `ipso.tgz` file to an FTP server or workstation.

You can now install IPSO 3.6 remotely from the FTP server or workstation. (See "Installing IPSO 3.6 from Command Shell or Voyager" on page 34.)

Using Nokia Horizon Manager to Install IPSO and Packages

You can use Nokia Horizon Manager v1.2 to automate the process of installing and upgrading IPSO 3.6 and software packages on multiple appliances. Use the OS Install action to install IPSO 3.6 on as many as 2500 platforms in a single data set. Horizon Manager v1.2 also provides actions that automate the installation and upgrade of software packages, such as Check Point NG FP2.

See the Horizon Manager v1.2 documentation for detailed information about the installation and upgrade process.

Before You Install IPSO from Command Shell or Voyager

Before you can install IPSO you must put the file `ipso.tgz` on your appliance. You can download this file to your appliance from an FTP server and perform the installation at one time, or you can first FTP the file to the appliance and then perform the installation.

Caution
If you perform a fresh installation of IPSO, you must download `ipso.tgz` and perform the installation at one time. Do not copy the `ipso.tgz` to the appliance first—it will be overwritten during the installation procedure. For more information, see "Overwriting Existing Images (Fresh Installation)" on page 38.

Using an FTP Server

To download IPSO 3.6 from an FTP server, insert the CD-ROM into the CD drive of the FTP server. If you are using a Unix FTP server, mount the file system. If you are using a Windows NT FTP server, copy `ipso.tgz` and any appropriate package files to an FTP directory.

To install IPSO 3.6 directly from the FTP server, go to "Installing IPSO 3.6 from Command Shell or Voyager" on page 34. If you want to copy `ipso.tgz` to your appliance and then perform the installation, proceed to the following section.

Copying IPSO 3.6 to Your Appliance (Optional)

Copying IPSO 3.6 to your appliance allows you to perform a local installation (as opposed to a remote installation from an FTP server).

1. Use Nokia Network Voyager to enable FTP access to the appliance. To do so:
   a. On the Voyager home page, click *Config*.
   b. In the *Security and Access Configuration* section, click the *Network Access and Services* link.
   c. In the *Allow FTP access* field, click *Yes*.
   d. Click *Apply*
   e. Click *Save* to make your change permanent.

2. To copy IPSO 3.6 from a workstation:
   a. Insert the CD-ROM into the CD drive of the workstation.
   b. Make sure that you can connect to the Nokia appliance over the network.
3. Open the directory on the FTP server or workstation that contains `ipso.tgz` (this can be the `image` directory on the CD-ROM).
4. Begin an FTP session to your appliance.

   By default, the current directory should be `var/admin`. Do not change the current directory.
5. At the prompt, enter

   `bin`
6. Transfer `ipso.tgz` to the appliance. At the prompt, enter

   `put ipso.tgz`
7. Close the FTP session.

Verifying MD5 Values

If you originally downloaded IPSO 3.6 from the Nokia support site, use the MD5 application to check that the file did not change during the download process.

1. Log on to the appliance through a console connection.
2. At the prompt, enter

   `md5 nkipflash.bin.`

   You should see a response that displays the same MD5 value that you copied from the support site. For example, you should see something like

   `MD5 (nkipflash.bin) = 1b248152586d0599e27130b1251c38c6`

Note
The preceding MD5 value is an example only. You will see a different value.

3. Compare the MD5 value you see to the value posted on the Nokia support site.

   If the values are identical, the download was successful and the file is good. If not, download the file (in binary) again and repeat this procedure.

To complete your installation of IPSO, proceed to the following section.

Installing IPSO 3.6 from Command Shell or Voyager

Note
If you intend to upgrade Check Point VPN-1/FireWall-1, do so before you upgrade IPSO. See "Upgrading to Check Point VPN-1/FireWall-1 NG FP2 with the IPSO Command Shell" on page 47.

You can change the version of IPSO running on your appliance in either of the following ways:

- You can add the new version of IPSO (also known as an IPSO image) without removing the existing images or your configuration information. If you add a new version, you can easily revert to the earlier versions stored on the appliance. When you do so, your configuration information is not affected.
- You can perform a fresh installation, which removes the existing images and your configuration information. If you perform a fresh installation, you can revert to versions of IPSO that were previously installed, but the process is more involved and all of your configuration information is removed again.

Note
When you add an image or perform a fresh installation using the IPSO command shell, use a console connection (rather than telneting to an interface that is already configured).

Adding an IPSO Image Using Voyager

Note
If you intend to upgrade Check Point VPN-1/FireWall-1, do so before you upgrade IPSO. See "Upgrading to Check Point VPN-1/FireWall-1 NG FP2 with the IPSO Command Shell" on page 47.

The instructions for adding an image using Voyager are in the Voyager online documentation. To see the instructions, follow these steps:

1. On the Voyager home page, click *Doc*.
2. Click *System Configuration*.
3. Scroll down to the section Installing New IPSO Images and click *Upgrading the IPSO Image.*

Adding an IPSO Image from the Command Shell

This section describes how to install IPSO by using the IPSO command shell over a console connection. For instructions about how to install IPSO using the CLI, see the *CLI Reference Guide for IPSO 3.6*, which is included on the documentation CD that comes with your appliance.

To add a new image from the IPSO command shell, use the `newimage` command. The syntax is

```
newimage [[-i | -l local_file] [-b] [-R | -T]] [-r | -t
image_name]
[-k] [-v]
```

Table 2 describes the options you can use with the `newimage` command.

Table 2 newimage options

`-i`	Load a new image interactively. Interactive mode supports anonymous FTP, FTP with a user name and password, access to a CD-ROM (IP440 only), and access to the local file system.
`-l local_file`	Extract the new image from a local file.
`-b`	Force upgrade of boot manager.
`-R`	Use newly installed image at next reboot.
`-T`	Test boot using newly installed image (not supported on IP440).
`-r image_name`	Specify image to run at next boot.
`-t image_name`	Specify image to run at next test boot (not supported on IP440).
`-k`	Do not deactivate existing packages. The `-k` option keeps 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 continues to do so. (The default is for all packages to be disabled by the `newimage` command.)
`-v`	Verbose FTP.

Note
You must reboot your appliance after you use the `newimage` command to upgrade the IPSO image. Save your current configuration before installing the new image.

Follow this procedure to add an IPSO image.

1. Log on to your appliance using a console connection.

Note
If you originally downloaded IPSO 3.6 from the Nokia support site, use the MD5 application to check that the file did not change during the download process. (See "Verifying MD5 Values" on page 33.)

2. Perform one of the following, depending on whether you copied `ipso.tgz` to your appliance or will install it from an FTP server:
   - If the IPSO image is copied to your appliance, enter

     `newimage -k -l ipso.tgz`

     You should see a response similar to the following:

     ```
     ipso.tgz Validating image...done.
     Version tag stored in image: IPSO-3.6-FCS1-releng 849
     02.12.2001-102644
     Installing new image...done [example]
     ```

   - If the IPSO image is on an FTP server, enter

     `newimage -i -k`

     The installation procedures prompt you for the IP address of the FTP server and the path to the ipso.tgz file.
3. Reboot your appliance when prompted.

Overwriting Existing Images (Fresh Installation)

Caution
The following procedure deletes any existing images and configuration information on your appliance. Back up any files that you want to keep and copy them back to the appliance after you install the new system. Nokia does not guarantee that any configuration files from the previous version of IPSO will work with the new version of IPSO.

Before you begin, make sure that you know:

- The serial number of your appliance. The number is on a sticker attached to the appliance and is preceded by "S/N."
- Whether the appliance will run IGRP.
- Whether the appliance will run BGP.
- An IP address that you will assign to the appliance.
- The appropriate network mask length.
- The IP address of the FTP server.
- The path to `ipso.tgz` on the FTP server.
- The IP address of the default gateway for the appliance.
- A host name to assign to the appliance.
- An appropriate password to assign to the administrator account.

The following sections describe a fresh installation of the IPSO image using the `install` command. The procedure differs depending on your appliance.

To perform a fresh installation on an IP440, see "Fresh Installation on the IP440" on page 41.

To perform a fresh installation on an appliance other than the IP440, go to the following section.

Fresh Installation on Appliances Other Than IP440

1. Log on to your appliance through a console connection.
2. At the prompt, enter **reboot**.
3. When the system enters autoboot mode and displays the message

   ```
   Type any character to enter command mode
   ```

   press any key to display the boot manager prompt.
4. At the boot manager prompt, enter **install**.

   If a password is configured, the system prompts you to enter the boot manager password.
5. The installation script runs.

   Follow the steps to install the new IPSO image from an FTP server.
6. At the end of the installation procedure, enter **reboot**.
7. After your appliance reboots, follow the prompts to configure basic settings.
8. When you see the message

   ```
   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 ]:
   ```

   type 1. Do not type 2. (The Lynx browser does not start properly at this point. For more information, see “Lynx Will Not Start” on page 64.)
9. When you see the message

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

   choose y (the default option). If you choose n, you cannot use Voyager unless you do one of the following:

   - Perform the installation procedure again and set a default route.

- Use the command-line interface to create a default route or static route.

10. When you see the message

```
Modem detected on /dev/cuaa1.
Enable logins on this modem [y,n]:
```

do not be concerned if a modem is not installed in your appliance. Type n and continue.

11. If there is a modem installed on this port (COM1—the external serial port on the front of the appliance), you can type y. If you do so, you are also asked if you want to set the country code on the modem. Type n in response to this question—use Voyager if you want to configure country codes for the external modem. Note that you cannot configure a country code on an IP330. If there is a PC card (PCMCIA) modem installed in the appliance, you see the message

```
Modem detected on /dev/cuaa3.
Enable logins on this modem [y,n]:
```

(The message says `cuaa4` if the modem is installed in COM4.)

Type y if you want to enable logins on the modem.

12. If you enable logins on a PC card modem, you are also asked if you want to set the country code on the modem.

- If you want to configure a country code and know the appropriate code, you can type y and then enter the code when prompted.
- If you do not want to configure a country code or if you do want to configure one but don't know the appropriate code, type n. You can use Voyager later to learn and configure the correct country code.

Note that you cannot configure a country code on an IP330.

13. When you are prompted to log into the appliance, you are ready to continue configuring your appliance. You probably want to do one of the following:

- Log into the appliance and then use the `newpkg` command to install packages. For more information, see "Using the newpkg Command" on page 46.
- Use Voyager to complete the configuration (including installing packages). To log in using Voyager, put the IP address you configured for the appliance in the URL field of your browser.

Fresh Installation on the IP440

When you perform a fresh installation of IPSO on an IP440, the installation procedure differs slightly depending on whether you install IPSO from an FTP server or the CD-ROM.

Caution
This procedure deletes any existing images and configuration information on your appliance. Back up any files that you want to keep and copy them back to the appliance after you have installed the new system. Nokia does not guarantee that any configuration files from the previous version of IPSO will work with the new version of IPSO.

IPSO on FTP Server

Use the following procedure to perform a fresh installation when `ipso.tgz` is on an FTP server.

1. Insert the boot disk into the appliance disk drive.
2. Boot the appliance.
3. The installation script runs. Follow the prompts to install the new IPSO image from an FTP server.
4. At the end of the installation procedure, enter **`reboot`**.
5. After your appliance reboots, follow the prompts to configure basic settings.

6. When you see the message

```
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 ]:
```

type 1. Do not type 2. (The Lynx browser does not start properly at this point. See "Lynx Will Not Start" on page 64 for more information.)

7. When you see the message

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

choose y (the default option). If you choose n, you will not be able to use Voyager unless you do one of the following:

- Perform the installation procedure again and set a default route.
- Use the command-line interface to create a default route or static route.

8. When you see the message

```
Modem detected on /dev/cuaa1.
Enable logins on this modem [y,n]:
```

do not be concerned if a modem is not installed in your appliance. Type n and continue.

9. When you are prompted to log into the appliance, you are ready to continue configuring your appliance. You probably want to do one of the following:

- Log into the appliance and then use the `newpkg` command to install packages. See "Using the newpkg Command" on page 46 for more information.
- Use Voyager to complete the configuration (including installing packages). To log in using Voyager, put the IP address you configured for the appliance in the URL field of your browser.

IPSO on CD-ROM

Use the following procedure to perform a fresh installation when you install `ipso.tgz` directly from the CD-ROM.

Note
While the installation or setup program is running, you cannot remove the CD-ROM. Ensure you have the proper CD-ROM in the system before starting.

1. Insert the CD-ROM into the appliance CD-ROM drive.
2. Insert the boot disk into the appliance's floppy disk drive.
3. Boot the appliance.
4. The installation script runs. Enter the required information at the prompts.
5. When you are prompted for the installation method, type 1 to install from the CD-ROM.
6. When you are prompted for the path to `ipso.tgz` and the name of the image file, press Enter to accept the default values.
7. When prompted, remove the boot disk and reboot the system.

From this point, the CD-ROM installation proceeds from step 5 on page 41.

Installing and Activating Packages

After you install IPSO, you may want to install Nokia documentation and third party packages (for Check Point VPN-1/FireWall-1 NG, for example). If you added a new version of IPSO using `newimage` and the `-k` (keep) option, your previous packages are active with the new IPSO version. If you used `newimage` without `-k` option, all the optional packages currently installed on the appliance are turned off, but they are not deleted. To turn these packages on again, see "Activating Packages" on page 45.

If you performed a fresh installation of IPSO, you must install and activate the packages you want to use. You can do this using Horizon Manager, Voyager, the command-line interface (CLI), or the `newpkg` command at the IPSO command shell.

For information about using the CLI to install and activate packages, see the *CLI Reference Guide for IPSO 3.6*, which is on the documentation CD that came with your appliance. You can also get the *CLI Reference Guide* by clicking *Doc* on the Voyager home page or visiting the Nokia customer support web site. For information about using Horizon Manager to install and activate packages, see the *Horizon Manager User's Guide*.

For information about the `newpkg` command, see "Using the newpkg Command" on page 46. For information about how to install packages, see the following section.

Using Voyager to Install Packages

To install Nokia documentation and third party packages using Voyager, perform the following procedure:

1. Log on to your appliance using Nokia Network Voyager.
2. On the Voyager home page, click the *System Configuration* link.
3. Click *Manage Installed Package*s.
4. Click *FTP and Install Package*s.
5. Enter the name or IP address of the FTP server.
6. Enter the path to the directory on the FTP server where the packages are stored.
7. If necessary, enter the appropriate user name and password.
8. Click *Apply.*

   The names of the available packages appear in the Site Listing window.
9. Select the packages you want to install.
10. Click *Apply.*

The selected package is downloaded to the appliance. When the download is complete, the package appears in the Unpack New Packages field.

11. Select the package in the Unpack New Packages field.
12. Click *Apply.*
13. Click the link to install/upgrade the package.
14. (Optional) To display all installed packages, click Yes next to Display all packages; then click *Apply.*
15. (Optional) To perform a first-time installation, click Yes next to Install; then click *Apply.*
16. (Optional) To upgrade a package, Click Yes next to Upgrade.
17. (Optional) To upgrade a package, click the button of the package from which you want to upgrade under Choose one of the following packages to upgrade from.
18. Click *Apply.*
19. Click *Save* to make your changes permanent.

Activating Packages

To turn on optional packages that were deactivated when you added a new version of IPSO using `newimage`, perform the following procedure.

1. Log on to the appliance using Nokia Network Voyager.
2. On the Voyager home page, click the *System Configuration* link.
3. Click *Manage Installed Package*s.
4. Click On next to the packages you want to turn on.
5. Click *Apply.*
6. Click *Save*.
7. Reboot your appliance.

Your installation of IPSO 3.6 is complete, and the packages that you selected are activated.

Using the newpkg Command

Use the `newpkg` command to add documentation and third party packages. To use the configuration files from a previously installed version of a package, use Voyager to upgrade the package.

The syntax of `newpkg` is

```
newpkg [-d] [-h] [i] [-l user_name] [-m media_type] [-n
path]
[-o path] [-p password] [-s server_ipaddrs] [-S] [-v]
```

Table 3 describes the options you can use with the `newpkg` command.

Table 3 newpkg options

`-d`	Print debug messages.
`-h`	Display help lines for command-line parameters.
`-i`	Install only (do not activate).
`-l user_name`	User name for FTP.
`-m media_type`	Media type; for example, FTP, CD, and so on.
`-n path`	Full path to new package.
`-o path`	Full path to old package for upgrade.
`-p password`	Password for FTP.
`-s server_ipaddrs`	The server IP address if media type is FTP/AFTP.

`-S`	Silent mode. Silent mode requires the following options: `-o`, `-m`, `-n`. If the media type is FTP/AFTP, silent mode also requires `-s`. If the media type is FTP, silent mode also requires `-l`, `-p`.
`-v`	Verbose FTP.

Note
The `newpkg` command is automatically invoked if you perform a fresh installation. You are prompted to install or skip each package.

To turn on the installed packages, continue with the procedure in "Activating Packages" on page 45.

Upgrading to Check Point VPN-1/FireWall-1 NG FP2 with the IPSO Command Shell

Using the following procedure to upgrade VPN-1/FireWall-1 allows you to migrate configuration data to the new release and reboot your appliance only once. (You upgrade VPN-1/FireWall-1 before you upgrade IPSO.) This procedure also allows you to revert to the previous service pack.

Note
To run the Check Point and IPSO SNMP daemons simultaneously, do not start the Check Point SNMP daemon during the installation procedure.

1. Log on to your appliance console; at the prompt, enter **`newpkg`**.
2. Choose the installation method that allows you to upgrade from an FTP server.
3. The system prompts you to enter the pathname to the directory on your server that contains package files.

4. The system prompts you step-by-step to install VPN-1/FireWall-1.
5. Upgrade to IPSO 3.6. (See “Adding an IPSO Image from the Command Shell” on page 35.)
6. Reboot the system.

4 Limitations

Nokia wants to hear about information you might have regarding these limitations. Contact Customer Service at 1-650-625-2525 or email tac.support@nokia.com.

For a more comprehensive listing of resolutions to problems, see the online knowledge base at https://support.nokia.com. Consult the knowledge base occasionally because records are continually added after the completed cases are reported to the Customer Service Center.

The following section describes known limitations associated with IPSO 3.6.

VPN-1/FireWall-1 Related Limitations

This section explains several issues related to Check Point VPN-1/FireWall-1 Next Generation (NG).

FP2 Installs FP1

If you are upgrading from Check Point VPN-1/FireWall-1 NG FP1 to FP2, make sure that FP1 is active before you begin the upgrade process. If you do not do so, your configuration information will be lost and you will not be able to revert to FP1 should you want to.

The FP2 installation process will install FP1 if it isn't already present. After FP2 is installed, do not remove FP1. If you do so, some FP2 functionality will be disabled.

1. **`echo $CPDIR`**
2. **`cd`** *<directory that CPDIR is set to>*
3. **`./bin/snmpd -p 260`**

   This command starts the Check Point .

Multicast Routing with VPN-1/FireWall-1 NG

To route multicast packets in conjunction with VPN-1/FireWall-1 NG, you must enable a flag in VPN-1/FireWall-1 to allow packets that are directed to an unknown interface (unknown to VPN-1/FireWall-1, which does not recognize multicast interfaces). The default behavior in VPN-1/FireWall-1 is to drop all packets coming from or going to an unknown interface.

Note
You must obtain the modzap utility used in the following procedure from Nokia customer support.

To enable multicast routing with VPN-1/FireWall-1 NG, perform these steps:

1. In the IPSO command shell, enter

   ```
   modzap fw_allow_unknown_if $FWDIR/boot/modules/fwmod.o
   0x1
   ```

2. Restart your appliance.

To enable multicast routing, turn on and configure either Protocol-Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP). For more information, see the online documentation in Voyager.

Number of Supported Interfaces

Different versions of VPN-1/FireWall-1 support different numbers of interfaces. If you assign more interfaces than are supported (as might be the case in VLAN configurations), the additional interfaces are treated as unknown interfaces by VPN-1/FireWall-1 NG and can pose a security risk.

- VPN-1/FireWall-1 NG FP1 supports a maximum of 256 interfaces on Nokia systems.
- There is an update to VPN-1/FireWall-1 NG FP2 that allows it to support a maximum of 256 interfaces on Nokia systems. Without this update, FP2 supports a maximum of 64 interfaces on Nokia systems. The update of FP2 is available from Check Point (see www.checkpoint.com). It is not compatible with FloodGate-1, Real-time Monitor, and UserAuthority.

Clustering

The following sections explain issues related to firewall/VPN clustering configurations.

Stability Limitation

There is a limitation that affects the stability of clusters running VPN-1/ FireWall-1 NG FP2. VPN traffic with security associations of short duration can cause cluster nodes to leave the cluster and then rejoin it. Check Point has produced an update to FP2 that addresses this issue.

If you purchased a Nokia appliance with FP2 and IPSO 3.6 installed, this limitation does not apply—the version of FP2 on the appliance has already been updated.

If you downloaded IPSO 3.6 from the Nokia customer support site, you should go to www.checkpoint.com to obtain the update to FP2.

Cluster May Drop SecuRemote Connections

Firewall/VPN clusters that contain more than two nodes might drop existing SecuRemote connections under certain conditions. If there is a series of node failures within the cluster, an existing SecuRemote connection might get dropped after one of the failures.

This problem has not been observed in two-node firewall/VPN clusters.

Do Not Use Crossover Cable for Synchronization

Do not use a Ethernet crossover cable for the cluster synchronization connection (cluster primary and secondary interfaces) in a two-node cluster. Using a crossover cable will cause the cluster (both nodes) to stop forwarding traffic if either cluster synchronization interface stops functioning for any reason or if the crossover cable is disconnected from either interface.

Note
Use a network switch or hub to connect the cluster synchronization interfaces in a two-node cluster.

Online Documentation

The online documentation incorrectly states that FireWall-1 must be running before you can activate a cluster. If you do not want to enable FireWall-1 before activating a cluster, click *Yes* next to *Disable monitoring of FW-1/VPN-1 (for setup only)?* on the IPSO Cluster Configuration page in Voyager.

Note
Be sure to change this option to *No* after you finish configuring the cluster.

Disk Mirroring

The IP500 and IP700 Series appliances allow you to create disk mirror sets to protect against interruptions in service in the event that a disk drive fails. This section explains some details related to disk mirroring.

System Might Need to be Restarted

After you create a mirror set, you might need to restart the appliance to activate disk mirroring. If you use Nokia Network Voyager to create the mirror set, Voyager tells you to restart the system when it is necessary.

If you intend to use the CLI to create the mirror set, enter the following command at the IPSO command shell before you start the CLI:

```
disklabel -r wd0
```

You should see a response similar to the following:

```
8 partitions:
#        size    offset    fstype   [fsize bsize bps/cpg]
  a:    80325         0    4.2BSD        0     0     0   # (Cyl.    0 - 4)
  b:  2097152     80325      swap                         # (Cyl.    5 - 135*)
  c: 40188960         0    unused        0     0         # (Cyl.    0 - 2501*)
  d: 31745877   2996792    4.2BSD        0     0     0   # (Cyl.  186*- 2162*)
  e:  5446035  34742669    4.2BSD        0     0     0   # (Cyl. 2162*- 2501)
  f:   819315   2177477    4.2BSD        0     0     0   # (Cyl.  135*- 186)
  g:      256 40188704    mirror                         # (Cyl. 2501*- 2501*)
```

If you see a mirror partition listed, as in the last line of the output above, you do not need to restart the appliance. Follow the procedure below to create the mirror set. If you do not see a mirror partition listed in the output, perform this procedure and restart the appliance.

1. To start the CLI, enter

   ```
   clish
   ```

2. To create the mirror set, enter

   ```
   add diskmirror
   ```

Source Disk Cannot be Larger than Mirror Disk

You cannot create a mirror set in which the source disk is larger than the mirror disk. If you attempt to do so using Voyager, Voyager displays a disk geometry error message. You can create a mirror set in which the source disk is smaller than the mirror disk or the same size as the mirror disk.

Caution
Use only Nokia-supported hard disks as members of a mirror set.

The hard disks installed in Nokia appliances or supplied as field-replaceable units can vary—make sure that the source disk is smaller then the mirror disk or the same size as the mirror disk before you create a mirror set. You can determine the sizes of the disks by viewing the Disk Mirroring Configuration page in Voyager or Lynx. You can also use the CLI to determine the sizes of the disks. For more information, see the *CLI Reference Guide.*

The CLI does not provide any response if you attempt to create a mirror set in which the source disk is larger than the mirror disk. Therefore, if you are using the CLI and have any doubt about this issue, you should check the Disk Mirroring Configuration page in Voyager after you attempt to create the mirror set to see if any disk geometry errors are displayed. Voyager immediately displays an error message if there is a problem with the disk geometries.

Percentage of Synchronization

After you issue a command to create a mirror set, the system copies the contents of the source drive to the mirror drive. This process can take some time. If you are using Voyager and want to see the completion percentage, refresh your browser. Voyager shows how much of the contents of the source drive is copied to the mirror drive and an error message that says

```
Error: Mirror already present.
```

You can safely ignore this message.

When the completion percentage reaches 100 percent, disk mirroring is enabled.

Note
If the completion percentage never reaches 100 percent, the mirror drive is faulty and cannot be used. You must use a different drive to create a mirror set.

You can make configuration changes while synchronization is taking place. Be sure to click Save so that the changes are written to the source disk (and the mirror disk).

Downgrading, then Upgrading

If you upgrade to IPSO 3.6 from an earlier version, create a mirror set, and subsequently downgrade to an earlier version, you should be aware of the following:

- If you perform a fresh installation of the earlier version of IPSO (using the boot manager), the system asks if you want to create a mirror set. Do not choose to create a mirror set—versions of IPSO prior to 3.6 do not support disk mirroring.
- If you later upgrade from the earlier version of IPSO back to version 3.6, disk mirroring is automatically enabled and the disks appear to be synchronized. They are not completely synchronized however, because any configuration changes you made while using the earlier version of IPSO are not copied to the mirror disk. To use disk mirroring, delete the current mirror and create a new one.

IP530 Power Supply

If you want to create a disk mirror set on an IP530, you must make sure that the appliance has an appropriate power supply. While the power supply is installed in the appliance, determine if there is a part number label on the

supply's exterior. If there is, it is the appropriate power supply. If the power supply does not have a part number label its exterior it will not support disk mirroring and must be replaced. Contact Nokia to obtain a replacement.

IP700 Series Ethernet Ports

If you create a disk mirror set on an IP700 Series appliance, make sure that no traffic is coming into the built-in Ethernet ports ETH-3 and ETH-4 while the mirror set is being created. Deactivate these ports in Voyager or the CLI or physically disconnect them before you create the mirror set. If you do not deactivate them, the appliance might reboot while the mirror set is being created.

Once you determine (in Voyager or the CLI) that the disks are 100 percent synchronized, reactivate or reconnect ports ETH-3 and ETH-4.

Hot Swapping Disks and Disk Mirroring in IP700 Series

The IP700 Series of Nokia appliances supports disk mirroring and hot swapping of hard disk drives. "Hot swapping" refers to removing or installing a drive while the appliance is turned on.

Some restrictions apply to hot swapping, as explained in this section. If you read the rest of the section and determine that you can safely remove or insert a disk drive without turning off the power to your appliance, follow the instructions under "Hot Swapping a Disk Drive" on page 59.

Note
Nokia recommends that you start the system with the boot drive in slot A (labeled "HDD A" on the chassis). If you perform a fresh installation of IPSO to a system with one disk drive, install the drive in slot A.

System Allows Boot Drive to be Turned Off

If two disk drives are installed in an IP700 Series appliance and disk mirroring is not enabled, do not press the hot swap button next to the boot drive. If you do so, the system shuts off the power to this drive and the system fails.

Starting with Two Drives Installed

If you have two disk drives for your appliance, Nokia recommends that you start the system with both drives installed. Starting the system with this configuration allows you to remove and replace either hard drive without turning off the system (assuming that disk mirroring has been enabled and the drives are 100 percent synchronized).

Nokia also recommends that you start the system with the boot drive in slot A and the other drive in slot B (labeled “HDD B”).

System Does Not Start Properly

If the boot drive is installed in slot B and the drive in slot A is not functional to the extent that the system cannot communicate with it, the system does not start properly. In this circumstance, move the boot drive to slot A and install a new drive in slot B. Do not attempt to use the nonfunctional drive that was previously installed in slot A.

If the boot drive is installed in slot B and both of the following are true, the system does not start properly:

- A blank drive is installed in slot A.
- Disk mirroring is not enabled and was never enabled.

In this circumstance, you see the following messages in the IPSO command shell using a console connection:

```
Type any character to enter command mode.
/dev/wd0f on /mnt: Incorrect super block.
Error: /image on /dev/wd0f does not exist or is not a file
umount: /mnt: not currently mounted
boot failed
BOOTMGR[1]>
```

The system starts up if you remove the blank drive from slot A, but you cannot create a mirror set. The better approach is the following:

1. Turn the appliance off.
2. Move the boot drive to slot A.
3. Install the blank drive in slot B.
4. Restart the appliance.

Starting with One Drive Installed

If you start the appliance with only one drive installed, your ability to hot swap drives is affected by the location of the boot drive. (This is true even if you had previously operated the system with two drives installed and disk mirroring enabled.)

If the boot drive is installed in drive slot A, you can install a disk drive into slot B and remove it without turning off the appliance.

Note
Nokia recommends that you start the system with the boot drive in slot A.

If the boot drive is installed in drive slot B, you must turn the appliance off before you insert a disk drive into slot A. If you insert a drive into slot A without first turning off the appliance, the newly installed drive is not

recognized. This is true even if the boot drive in slot B was previously part of a mirror set.

Caution
If the boot drive is in slot B and you have hot swapped a drive into slot A, do not press the disk hot swap button next to slot B. If you do so, the system shuts off the power to drive B (the boot drive), and the system fails.

Hot Swapping a Disk Drive

Follow the instructions in this section to install or remove a disk drive in an IP700 Series appliance without turning off the power.

Note
Nokia recommends that you install the boot drive in slot A.

Removing a Disk Drive

1. Press the disk hot swap button next to the drive you want to remove.
2. Wait until both LEDs are off.
3. Loosen the thumbscrews and pull the drive out of the chassis.

Inserting a Disk Drive

1. Make sure that the top of the drive is facing up. (The manufacturer's label is on the top of the drive and a printed circuit board is visible at the bottom.)
2. Insert the drive all the way into the chassis.

   If you cannot push the drive all the way into the chassis, proceed to the next step.

3. Verify that the thumbscrews are aligned with their holes and tighten the screws.

   If necessary, use a Phillips-head screwdriver to tighten the thumbscrews.

4. Press the disk hot swap button.

   Verify that the Status LED is green to make sure that the drive is functional.

Message Displayed on Console

When you hot swap a disk drive into an IP700 Series appliance, you might see a message similar to the following on a console or telnet connection:

```
Adding Disk B
Mar 26 01:20:17 mirror [LOG_CRIT] kernel: Adding Disk B
wd2: interrupt timeout:
wd2: status 50<seekdone> error 1<no_dam>
wd2: wdtimeout() DMA status 4
Mar 26 01:20:28 mirror [LOG_CRIT] kernel: wd2: interrupt
timeout:
Mar 26 01:20:28 mirror [LOG_CRIT] kernel: wd2: status
50<seekdone> error 1<no_dam>
Mar 26 01:20:28 mirror [LOG_CRIT] kernel: wd2:
wdtimeout() DMA status 4
```

You can safely ignore this message.

Test Booting Images

After installing a different version of IPSO, you may want to test boot the appliance. After a test boot, you have several minutes to decide whether to continue using the newly booted IPSO image. If you do not commit to the new image within several minutes or if system does not start properly, the appliance reboots again and reverts to the previous version of IPSO.

If you want to download an IPSO image using the New Image Installation (Upgrade) page and then test boot the downloaded image, do not select the option Test Boot New Image option. Follow this procedure:

1. Enter the FTP URL of the IPSO image.
2. Select Existing Image.
3. Click *Apply.*

   Voyager displays the link New Image Installation Status.
4. Click New Image Installation Status.
5. When Voyager displays a message indicating that you should reboot the appliance, click *Manage IPSO Images (Including REBOOT).*
6. Select the image you want to test boot.
7. Click *Reboot*

Inaccurate Message After Halting

When you click *Halt* in Voyager to force an orderly shutdown of a Nokia appliance, you will see a message in the file /var/log/messages and in a console connection that indicates that the system is about to be rebooted. This message is inaccurate. The system will not restart unless you press any key while the console connection is active or manually turn the appliance off and on again.

CLI Limitations

This section explains some limitations of the IPSO command-line interface (CLI).

Repeated Ctrl-Cs May Cause Core Dump

When you enter a CLI command that produces more than one screen of output (such as `show route all`), the display stops scrolling when the window is full and the `-- More --` prompt is shown. If you enter a number of commands such as these and repeatedly press Ctrl-C when the `-- More --` prompt is displayed, the system may dump a core file and exit from the CLI. If there are any configuration changes that you have not saved (and that you want to save), follow these steps:

1. Restart the CLI by entering **`clish`**.
2. At the CLI prompt enter

   `save config`

Note
To avoid this issue, press q to return to the CLI prompt instead of Ctrl-C.

Monitoring Limitations

This section explains issues related to the monitoring features of IPSO 3.6.

Interface Throughput Reports

If you use the Interface Throughput Report page and choose settings that report very large numbers (billions) of packets or bytes of throughput, the graphical view will not display the throughput values on the y (vertical) axis. In this situation, you will also see a `masked floating point exceptions` error reported in the message log and in the IPSO command shell (telnet or console session).

You can see the throughput values by using the interface throughput report CLI commands. See the *CLI Reference Guide for IPSO 3.6* for more information.

Rate Shaping Bandwidth Reports

If you upgrade a Nokia appliance to IPSO 3.6, you might lose the ability to view rate shaping bandwidth reports for the time that the previous version of IPSO was active. This will be the case if all of the following are true:

- IPSO 3.3 was installed.
- The appliance was upgraded to a version between 3.3 and 3.6.
- The appliance is upgraded again to IPSO 3.6.

For example, if the appliance was first upgraded from IPSO 3.3 to 3.4, and then you upgrade it from 3.4 to 3.6, you will not be able to view rate shaping bandwidth data (in Voyager or the CLI) for the duration of the time that IPSO 3.4 was active.

This problem does not occur if you upgrade directly from IPSO 3.3 to 3.6, nor does it occur if you upgrade from a version later than 3.3, and 3.3 was never run on the appliance.

SNMP Limitations

This section explains issues related to IPSO 3.6 support for SNMP.

ISDN Pseudo Interfaces

An ifTable entry is shown for the following ISDN stack layers: ISDN Physical, ISDN Connection (logical), ISDN D Channel, and two ISDN B Channels. The ISDN Physical and ISDN Connection (logical) are real interfaces, while the ISDN D and two ISDN B channels are pseudo interfaces. The following limitation exists for the entries of the ISDN D and the two ISDN B channels in the ifTable:

- The ifLastChange object shows an incorrect value (0) when you change the state of the ISDN interface and when you hotswap the ISDN network interface card.

- The ifOperStatus object shows inconsistent values when the operational state of the ISDN interface is changed.

Objects Not in snmpwalk

The command `snmpwalk` will not find the following objects:

- ifTableLastChange
- ifStackLastChange

Support for RFC 1213 Deprecated

The MIB defined in RFC 1213 is deprecated in IPSO 3.6, but continues to be supplied with the system.

For more information on any supported MIB, see the /etc/snmp/mibs directory.

Lynx Will Not Start

Lynx is an ASCII-character based browser that you can use to configure your Nokia appliance if you do not want to use Nokia Network Voyager, the web-based browser. In a very specific circumstance, Lynx does not start properly.

If you install IPSO by using the boot manager to perform a fresh installation (that is, you overwrite the contents of the hard disk rather than adding an additional IPSO image), the system asks you to reboot it. After you do so, it asks you to provide a host name and password and then displays the following prompt:

```
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 ]:
```

If you enter `2`, the system displays

```
Do you wish to start Lynx now? [ y | n ]
```

If you type y, the system displays some messages and displays the IPSO command shell. It does not start Lynx. After the system displays the command line, you can start Lynx by entering **`lynx`**.

IP710, IP740 Issue

IP530 Issues

The issues described in this section are specific to the IP530 appliance.

Startup Error Message

You might receive the following error message when you reboot an IP530 appliance:

```
RTC BIOS diagnostic error 20
```

Ignore this message. It does not affect the operation of your appliance.

PCMCIA Modem

When you use the dialback option, make sure that the remote modem is set to auto-answer (S-register 0 is set to 1), because the auto-answer setting might not be the default setting for modems. In the IPSO command shell, type `ATS0=1` to set the modem for auto-answer.

When you use the dialback option, make sure that the remote modem baud rate is set correctly. For US Robotics external modems, type the command `AT&B1` to set the baud rate.

If the PCMCIA modem you are using was previously used on another device, the modem might have incorrect settings stored in the NVRAM-stored profile.

Check the settings by logging on to your appliance console and then using manual commands. Enter `tip modem` *`number`* where *`number`* is the port number where the modem is installed. Then type AT commands to check settings. To exit the tip program, type the tilde key and Ctrl-D.

Note
You must exit the `tip` program to enable dialin and dialback.

Note
To enable dialin and dialback options after overwriting an exiting IPSO image with a new IPSO image, you must run the `newsystem -f` command in addition to the steps outlined in "Overwriting Existing Images (Fresh Installation)" on page 38.

Using VRRP with Nortel or Extreme Switches

You can protect your network from failure by configuring two or more Nokia appliances to use the virtual router redundancy protocol (VRRP). If Nokia appliances running VRRP are connected to a network switch manufactured by Nortel or Extreme Networks, and you disable a port on the network switch using the switch's software interface, the Nokia appliance may not detect that the switch interface has been disabled. In this case, failover will not occur.

If you disable the link in hardware (for example, by removing the cable), the Nokia appliance will detect the failure and failover properly.

Inline Help Design

If you are using the a Netscape browser on a Unix system and you reload the pop-up window that contains the inline help, the original Voyager page reloads instead.

This behavior does not occur with any other browser on Unix systems or at all on Windows systems.

The pop-up help window was designed so that it cannot be resized. However, some window managers that are used with Free BSD allow you to resize this window.