Part No. 314997-B
April 2003

4655 Great America Parkway
Santa Clara, CA 95054

# Important Security Information for the 8000 Series Switch

NORTEL NETWORKS™

## Copyright © 2002 Nortel Networks



The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

## Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and [other Nortel trademarked product names] are trademarks of Nortel Networks.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

The asterisk after a name denotes a trademarked item.

# Contents

# Introduction

This booklet describes the security features available for your Passport 8000 Series Switch, and how to quickly disable non-secure protocols and configure your selected security feature(s). In order to maintain the security of your network, Nortel Networks recommends that you disable all non-secure protocols that could be used to communicate with the Passport 8000 switch. For further information about network security issues, see *Configuring and Managing Security, Passport 8000 Series Software Release 3.5* (part number 314724-B).

# Encryption notice

Currently DES (SNMPv3) and 3DES (SSHv1/v2) are the encryption algorithms supported for the Passport 8000 Series Switch. Due to export restrictions, the encryption capability has been separated from the main image. Refer to the upgrading documentation accompanying your software release for the latest information on how to download the encryption images. The SSH server and SNMPv3 protocol will not function properly without these images.

# Password encryption

In the Passport 8000 Series switch software release 3.5, passwords are stored in encrypted format and are no longer stored in the configuration file. If the switch is booted for the first time with the software release 3.5 image, the password is reset to default values and a log is generated indicating any changes.

**Note:** For security reasons, Nortel Networks recommends setting the passwords to values other than the factory defaults.

# Web server password and SNMP community string encryption

In the Passport 8000 Series switch software release 3.5, community strings are stored (as passwords have been since release 3.2.1) in encrypted format and are no longer stored in the configuration file. If a configuration file saved prior to release 3.5 is loaded, any saved community strings from the configuration file will not be recognized. If the switch is booted for the first time with the software release 3.5 image, the community strings are reset to default values and a log is generated indicating any changes.

**Caution:** For security reasons, Nortel Networks recommends that you set the community strings to values other than the factory defaults.

Web-server passwords and SNMP community strings are encrypted.

- Web-Server password

  The web-server passwords authenticate the user who is accessing the switch using the web interface. The passwords are encrypted using the blowfish algorithm and are stored in a hidden file. They are not visible on the switch through any **show** command and are not stored in the config file.

- SNMP community strings

  SNMP community strings are used when the user logs in to the switch over SNMP, for example, using Device manager. These strings are encrypted using the blowfish algorithm and are stored in a hidden file. They are not displayed on the switch and are not stored in the config file.

# Modifying and resetting passwords

The boot monitor command reset-passwd is introduced to reset the passwords to default values.

To reset the passwords, a boot monitor command `reset-passwd` is available.

To change the passwords use the following commands.

**Note:** All passwords are case sensitive.

```
config cli password <access-level> <username>

Enter the old password:

Enter the new password:

Re-enter the new password:
```

# Secure and non-secure protocols

Table 1 describes the secure and non-secure protocols.

**Table 1** Secure and non-secure protocols

| Non-secure protocols | Default status | Equivalent secure protocols | Default status |
|---|---|---|---|
| FTP/TFTP | Disabled | SCP | Disabled |
| Telnet | Enabled | Secure SHell (SSH) v1, v2 [1] | Disabled |
| SNMPv1, SNMPv2 | Enabled | SNMPv3 [2] | Enabled |
| Rlogin | Disabled | Secure SHell (SSH) v1, v2 [1] | Disabled |
| HTTP | Disabled | No equivalent [3] | |

1 Nortel Networks recommends that you use SSHv2 instead of SSHv1.

2 The DES image must be loaded on the switch to use SNMPv3.

3 Due to the risk to the security of your network, Nortel Networks recommends that you not use this protocol.

# Disabling non-secure protocols

To protect the security of your network, you should disable all of the non-secure protocols that could be used to gain unauthorized access to the Passport 8000 device. Each of the following sections describes typical applications for a non-secure protocol, and how to disable the protocol on the Passport 8000 device.

## Disabling Telnet

The telnet protocol is used to communicate with the switch for CLI operations. Telnet sessions over an open network can be easily intercepted, exposing passwords and user IDs. Once passwords and user IDs are known, unauthorized users can gain access to device configuration and disrupt or compromise network communication.

Use the following command to disable the Telnet protocol using the CLI interface:

```
config bootconfig flags telnetd false
```

## Disabling SNMPv1 or SNMPv2

The SNMPv1 and SNMPv2 protocols are used to communicate with the switch for device and network management operations by Java Device Manager and Optivity Switch Manager.

Use the following command to disable the SNMPv1 and SNMPv2 protocols using the CLI interface:

```
config bootconfig flags block-snmp true
```

## Disabling FTP/TFTP

The FTP and TFTP protocols are used to transfer configuration files to and from the Passport 8000 device.

Use the following command to disable the FTP and TFTP protocols using the CLI interface:

```
config bootconfig flags ftpd false
config bootconfig flags tftpd false
```

## Disabling HTTP

The HTTP protocol is used to communicate with the switch for operations by the built-in Web management server. The default setting for the Web management server is disabled.

If the Web management server has been enabled, you can use the following command to disable the HTTP protocol using the CLI interface:

```
config web-server disable
```

## Disabling Rlogin

The rlogin protocol is used to communicate with the switch for CLI operations. The default setting for the rlogin service is disabled.

If the rlogin service has been enabled, you can use the following command to disable the rlogin protocol using the CLI interface:

```
config bootconfig flags rlogind false
```

# Enabling secure protocols

Each of the following sections describes typical applications for a secure protocol, and how to enable the protocol on the Passport 8000 device.

## Enabling SSH and SCP

In order to enable the SSH and SCP protocols, you must load the DES encryption image into the Passport 8000 switch memory. You can obtain the DES encryption image from the Nortel Networks Web site. For more information configuring and enabling SSH and SCP, see “Configuring SSH” in *Configuring and Managing Security, Passport 8000 Series Software Release 3.5* (part number 314724-B).

Use the following CLI command to enable SSH and SCP:

```
config bootconfig flags sshd true
```

## Enabling SNMPv3

In order to enable the SNMPv3 protocol, you must load the DES encryption image into the Passport 8000 switch memory. You can obtain the DES encryption image from the Nortel Networks Web site. For more information configuring and enabling SNMPv3, see “Configuring SNMPv3” in *Configuring and Managing Security, Passport 8000 Series Software Release 3.5* (part number 314724-B).

## Securing the network management interface with access policies

You can use access policies to quickly secure the network access interfaces of the device. The following three sections show examples that demonstrate how you might quickly implement such policies. Bold courier text indicates command input. Normal courier indicates system responses. For detailed information about access policies, see *Configuring and Managing Security, Passport 8000 Series Software Release 3.5* (part number 314724-B).

After you create access policies, enable the access policy feature using the following command:

```
config sys access-policy enable true
```

## Denying network management access for a specific station

The following set of commands creates a policy that denies network access via the specified protocols to the specified host. This deny mode policy specifies addresses and services that are denied access to the switch.

```
NYK>:5# config sys access-policy policy 2
NYK>:5/config/sys/access-policy# policy 2
NYK>:5/config/sys/access-policy/policy/2# create
NYK>:5/config/sys/access-policy/policy/2# name POLICY2
NYK>:5/config/sys/access-policy/policy/2# mode deny
NYK>:5/config/sys/access-policy/policy/2# network 47.81.113.152/32
NYK>:5/config/sys/access-policy/policy/2# host 47.81.113.152
NYK>:5/config/sys/access-policy/policy/2# precedence 1
NYK>:5/config/sys/access-policy/policy/2# service
NYK>:5/config/sys/access-policy/policy/2/service# http enable
NYK>:5/config/sys/access-policy/policy/2/service# rlogin enable
NYK>:5/config/sys/access-policy/policy/2/service# snmp disable
NYK>:5/config/sys/access-policy/policy/2/service# telnet disable
NYK>:5/config/sys/access-policy/policy/2/service# tftp enable
NYK>:5/config/sys/access-policy/policy/2/service# ftp enable
NYK>:5/config/sys/access-policy/policy/2/service# ..
NYK>:5/config/sys/access-policy/policy/2# ..
NYK>:5/config/sys/access-policy#
```

## Allowing network management access for a specific station

The following set of commands creates a policy that allows access to the switch for the specified station. However, it only allows access via SNMP and telnet services.

```
NYK>:5/config/sys/access-policy# policy 3
NYK>:5/config/sys/access-policy/policy/3# create
NYK>:5/config/sys/access-policy/policy/3# name POLICY3
NYK>:5/config/sys/access-policy/policy/3# mode allow
NYK>:5/config/sys/access-policy/policy/3# network 47.81.113.152/32
NYK>:5/config/sys/access-policy/policy/3# host 47.81.113.152
NYK>:5/config/sys/access-policy/policy/3# precedence 10
NYK>:5/config/sys/access-policy/policy/3# service
NYK>:5/config/sys/access-policy/policy/3/service# http disable
NYK>:5/config/sys/access-policy/policy/3/service# rlogin disable
NYK>:5/config/sys/access-policy/policy/3/service# snmp enable
NYK>:5/config/sys/access-policy/policy/3/service# telnet enable
NYK>:5/config/sys/access-policy/policy/3/service# tftp disable
NYK>:5/config/sys/access-policy/policy/3/service# ftp disable
NYK>:5/config/sys/access-policy/policy/3# network 47.81.113.152/32
NYK>:5/config/sys/access-policy/policy/3# host 47.81.113.152
NYK>:5/config/sys/access-policy/policy/3# ..
NYK>:5/config/sys/access-policy#
```

## Denying network management access for all stations

The following set of commands creates a default policy denies access to the switch via any of the unsecured network management protocols.

```
NYK>:5/config/sys/access-policy# policy 1
NYK>:5/config/sys/access-policy/policy/1# mode deny
NYK>:5/config/sys/access-policy/policy/1# service
NYK>:5/config/sys/access-policy/policy/1/service# rlogin enable
NYK>:5/config/sys/access-policy/policy/1/service# snmp enable
NYK>:5/config/sys/access-policy/policy/1/service# telnet enable
NYK>:5/config/sys/access-policy/policy/1/service# tftp enable
NYK>:5/config/sys/access-policy/policy/1/service# ftp enable
```

## Using route policies to restrict route distribution

The Passport 8000 switch has a rich set of IP and IPX policies that you can use to restrict the announcement of IP and IPX routes within your network and also restrict access to portions of your network. For more information about IP and IPX route policies, see *Configuring IP Routing Operations* (part number 314720-C) and *Configuring IPX Routing Operations* (part number 314722-A).

## Secure routing protocols

You can configure your network so that OSPF updates are protected by an MD5 key on each interface, as described in RFC2178 (OSPF cryptographic authentication with the MD5 algorithm). Using a similar MD5 scheme, you can secure BGP updates as described in RFC2385.

For more information about route update protection, see *Configuring Network Management, Passport 8000 Series Software Release 3.5* (part number 314723-B).