Sun™ N2000 Series Release 2.0.6 —Release Notes

Sun Microsystems, Inc.
www.sun.com
Part No. 817-7639-15
February 2006, Revision A

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Please
Recycle

Adobe PostScript

Regulatory Compliance Statements

Your Sun product is marked to indicate its compliance class:

- Federal Communications Commission (FCC) — USA
- Industry Canada Equipment Standard for Digital Equipment (ICES-003) — Canada
- Voluntary Control Council for Interference (VCCI) — Japan
- Bureau of Standards Metrology and Inspection (BSMI) — Taiwan

Please read the appropriate section that corresponds to the marking on your Sun product before attempting to install the product.

FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

ICES-003 Class A Notice - Avis NMB-003, Classe A

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

ICES-003 Class B Notice - Avis NMB-003, Classe B

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

VCCI 基準について

クラス A VCCI 基準について

クラス A VCCI の表示があるワークステーションおよびオプション製品は、クラス A 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

クラス B VCCI 基準について

クラス B VCCI の表示  があるワークステーションおよびオプション製品は、クラス B 情報技術装置です。これらの製品には、下記の項目が該当します。

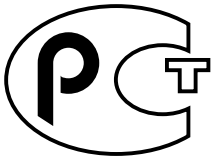
この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

BSMI Class A Notice

The following statement is applicable to products shipped to Taiwan and marked as Class A on the product compliance label.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用
時，可能會造成射頻 干擾，在這種情況下，
使用者 會被要求採取某些適當的對策。

GOST-R Certification Mark



Declaration of Conformity

Compliance Model Number: N2040_N2120
Product Name: Sun N2000 Series

EMC

USA—FCC Class B

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This equipment may not cause harmful interference.
2. This equipment must accept any interference that may cause undesired operation.

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001)		Required Limits:
	EN55022/CISPR22	Class B
	EN61000-3-2	Pass
	EN61000-3-3	Pass
	EN61000-4-2	6 kV (Direct), 8 kV (Air)
	EN61000-4-3	3 V/m 80-1000 MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
	EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
	EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
	EN61000-4-6	3 V
	EN61000-4-11	Pass

As Information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997		Class B
EN55024:1998 Required Limits:		
	EN61000-4-2	4 kV (Direct), 8 kV (Air)
	EN61000-4-3	3 V/m
	EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
	EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines, 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
	EN61000-4-6	3 V
	EN61000-4-8	1 A/m
	EN61000-4-11	Pass
	EN61000-3-2	Pass
	EN61000-3-3	Pass

Safety

This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN60950:2000, 3rd Edition	TÜV Rheinland Certificate No. S 72042727
EN60950:1999, 3rd Edition, Evaluated to all CB Countries	CB Scheme Certificate No US-TUVR-2047
UL 60950:2000 3rd Edition: 2000, CSA C22.2 No 60950-00	File: E234800-A1-UL-1

Supplementary Information: This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski DATE
Manager, Compliance Engineering
Sun Microsystems, Inc.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054 USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Donald Cameron DATE
Program Manager
Sun Microsystems Scotland, Limited
Blackness Road, Phase I, Main Bldg.
Springfield, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 539
Fax: +44 1 506 670 011

Contents

Sun N2000 Series Release 2.0.6 Release Notes

Introduction 1-1
Related documentation 1-2
Product Web page 1-2
Obtaining patches from Sun 1-3
Contacting Sun technical support 1-3
Sun welcomes your comments 1-3
Third-party Web sites 1-4
Abbreviations and Acronyms 1-4
Configuration Instructions 1-4
- Archiving a Version 2.0 Configuration 1-4
- How to Import Archived Configurations Into a New Switch 1-5
- How to Remove the Existing Switch Configuration 1-7
- How to Define the Management Address and Default Gateway 1-8

Enhancements 1-9
- ACL Route Action 1-9
- Client Address Translation 1-10

Supported hardware 1-10
- Interface support 1-12

Operational considerations 1-12
- Fiber-optic transceivers 1-12

Software Information 1-13
- System installation and startup 1-13
- System configuration file 1-13

Management support 1-13

Command-line interface 1-13
Web interface 1-14
SNMP 1-15
Configuration scaling 1-15
Known problems, restrictions, and limitations 1-17
Documentation updates 1-21
Manuals 1-22
Online Help 1-24

Sun N2000 Series Release 2.0.6 Release Notes

Introduction

The *Sun N2000 Series Release 2.0.6 – Release Notes* supports the Sun™ N2000 Series Release 2.0, which includes both hardware and software. The Sun N2000 Series system is an intelligent application switch that provides advanced Secure Sockets Layer (SSL) acceleration with reencryption and advanced Layer 4 to Layer 7 (L4 to L7) load balancing. The Sun N2000 Series system provides these services on a flexible, virtualized basis, within the convenience of a single enclosure, and with industry-leading speed, security, and availability. The N2000 Series comprises the N2040 switch and the N2120 switch. When it is necessary to differentiate between the two switches, the model numbers are used in this manual.

This manual may refer to the Sun N2000 Series system as the “N2000 Series,” the “application switch,” the “switch,” or the “system.”

Related documentation

For complete information about the Sun N2000 Series system, see the following documents.

Title	Part Number	Location
Sun N2000 Series Release 2.0 — Introduction Guide	817-7641	Online Documentation CD
Sun N2000 Series Release 2.0 — Quick Installation	817-7640	Online Printed, in ship kit Documentation CD
Sun N2000 Series Release 2.0 — Hardware Installation and Startup Guide	817-7638	Online Printed, in ship kit Documentation CD
Sun N2000 Series Release 2.0 — System Configuration Guide	817-7637	Online Documentation CD
Sun N2000 Series Release 2.0 — System Administration Guide	817-7635	Online Documentation CD
Sun N2000 Series Release 2.0 — Command Reference	817-7636	Online Documentation CD
Sun N2000 Series Release 2.0.6 — Release Notes (This document)	817-7639	Online Printed, in ship kit

Product Web page

For access to the most up to date information about the N2000 Series product, including the most updated documentation, go to the following Web site:

http://www.sun.com/products/networking/switches

Obtaining patches from Sun

You can obtain patches from your Sun authorized sales representative, service provider, or by downloading them from the SunSolve Online℠ Web site at the following URL:

http://sunsolve.sun.com

For patch information instructions, see the README file that accompanies each patch.

Note: If you were provided a point patch (a temporary fix provided by engineering that is now part of an official release), you must remove the point patch files prior to installing an official patch release.

Contacting Sun technical support

If you have technical questions about this product that are not answered in this document, go to:

http://www.sun.com/service/contacting

Sun welcomes your comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

http://www.sun.com/hwdocs/feedback

Please include the title and part number of your document with your feedback:

Sun N2000 Series Release 2.0.6 – Release Notes, part number 817-7639-15

Third-party Web sites

Sun is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Abbreviations and Acronyms

Refer to the other Sun N2000 Series documents for definitions of industry-standard and product-specific abbreviations and acronyms used in these Release Notes.

Configuration Instructions

The following instruction sets describe how to archive, import, and remove 2.0 Switch Configurations.

Archiving a Version 2.0 Configuration

You can copy your configuration file for backup or archive purposes. To make a "portable" configuration file, use the `show runningConfig` command. Be sure to enable the `nameValuePairs` option, similar to the following:

```
sun(config)# show runningConfig saveToFile <myConfig.txt>
password <myPassword> nameValuePairs true
```

Perform the manual edits detailed below:

1. **Remove any lines for TCP connections.**

   These lines might appear multiple times, since this action happens once for each vRouter. The following is an example of what requires deletion:

```
#
# TCP Connections
#
tcp connections localAddress 0.0.0.0 localPort 22
remoteAddress 0.0.0.0 remotePort 0 state listen
```

```
tcp connections localAddress 0.0.0.0 localPort 23
remoteAddress 0.0.0.0 remotePort 0 state listen

tcp connections localAddress 0.0.0.0 localPort 80
remoteAddress 0.0.0.0 remotePort 0 state listen

tcp connections localAddress 0.0.0.0 localPort 443
remoteAddress 0.0.0.0 remotePort 0 state listen

tcp connections localAddress 10.8.170.123 localPort 23
remoteAddress 129.148.185.228 remotePort 1516 state
established
```

2. **Remove any lines for SSHd sessions.**

   The following is an example of what requires deletion:

```
#
# SSH sessions
#
sessions clientIp 129.148.30.128 clientPort 33127 sesStatus
active

sessions clientIp 129.148.30.128 clientPort 33127

exit;

sessions clientIp 129.148.30.165 clientPort 41440 sesStatus
active

sessions clientIp 129.148.30.165 clientPort 41440

exit;
```

You may now import this configuration to another switch running Version 2.0 software.

Note: For Redundant Config, you must manually remove the HTTPS management certificate before performing the tasks described above.

How to Import Archived Configurations Into a New Switch

This procedure enables you to apply a saved configuration to a new switch. Each configuration has switch chassis dependencies that may hinder the successful import. You must follow these steps in the specific order to successfully import a configuration into a new switch.

To complete this procedure, you need to have the following available:

- FTP server
- PC or workstation
- Management Ethernet access
- Console access
- Archived configuration file from the original switch

Note: You must run the command `show runningConfig saveToFile <filename> password <password>` on the original switch and copy the file to the FTP server before starting this procedure.

You must do the following to complete this procedure:

- Verify or install a Virtualization key
- Define the Ethernet IP address, mask, and gateway of the switch
- Use FTP to load the configuration file onto the switch
- Import the configuration file

Procedure

To import an archived configuration into a new switch, do the following:

1. **Connect your PC or workstation serial port to the switch's console port, using the cable supplied with the product.**
2. **Connect the Ethernet management port to a common IP network so that you can access the FTP server.**
3. **Connect to the switch's console port, using a terminal emulator.**
4. **Log in to the switch using the user name and password of `admin`:**

```
username: admin
password: admin
sun>
```

Note: You are now prompted to run the Setup utility. Do not run the Setup utility at this point. If you are not prompted to run the Setup utility now, complete the procedure in the section, "How to Remove the Existing Switch Configuration" first. Then, log back in to the switch and continue with Step 5 of this procedure.

5. **Enter the config mode:**

```
sun> enable
sun# config
sun(config)#
```

6. **Verify that the Virtualization key is installed:**

```
sun(config)# show switchServices software key
```

7. **If the Virtualization key is not installed, install the key:**

```
sun(config)# switchServices software key
<xx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx>
```

Note: The Virtualization key must be in the format `xx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx`, with all letters lowercase.

You have to define an IP host address and default gateway. If you have an FTP server available for your network, you can use the default IP setting of `10.10.1.1` and continue with the next step. If you cannot do this, complete the procedure in the section, "How to Define the Management Address and Default Gateway" first. Then, continue with Step 8 of this procedure.

8. **Enter the switchServices FTP client and log in to the FTP server:**

```
sun(config)# switchService ftp
sun(config-switchServices ftp)# open <ip address of ftp server>
<username> <password>
sun(config-switchServices ftp)# get <saved configuration file name>
sun(config-switchServices ftp)# close
sun(config-switchServices ftp)# exit
sun(config-switchServices)# exit
sun(config)#
```

9. **Enter the following command to import the saved configuration:**

```
sun(config)# import runningConfig fromFile <saved configuration
file name> password <password> stopOnError false
```

10. **Save the configuration:**

```
sun(config)# saveCfg
```

How to Remove the Existing Switch Configuration

To remove an existing configuration from a switch, perform the following steps:

1. **Enter the config mode:**

```
sun> enable
```

```
sun# config
sun(config)#
```

2. **Remove the existing configuration:**

```
sun(config)# switchServices software removeCfg

WARNING: This will permanently remove the configuration database
files from the flash file system. Reboot the switch before
executing the saveCfg command to use the factory default
configuration.

Do you wish to continue? (y or n): y
```

3. **Restart the switch:**

```
sun(config)# switchServices reset

WARNING: Restarting the Sun Application Switch will power down the
switch, interrupting all services.

Do you wish to continue? (y or n): y
```

Any existing configuration is removed. Return to Step 5 in the procedure, "How to Import Archived Configurations Into a New Switch."

How to Define the Management Address and Default Gateway

To verify and define the host address and default gateway, perform the following steps:

1. **Define the management Ethernet IP address:**

```
sun(config)# vSwitch system vRouter management
sun(config-vSwitch-system vRouter-management)# ip
sun(config-vSwitch-system vRouter-management ip)# address ifName
ethMgmt.1 <ip address> netMask <mask>
```

2. **Define the default gateway IP address:**

```
sun(config-vSwitch-system vRouter-management ip)# route static
0.0.0.0 mask 0.0.0.0 nextHop <ip address of the gateway>
```

3. **Force the default gateway entry:**

```
sun(config-vSwitch-system vRouter-management ip)# interface
ethMgmt.1 adminState disabled
```

```
sun(config-vSwitch-system vRouter-management ip)# interface
ethMgmt.1 adminState enabled
```

4. **Exit the configuration:**

```
sun(config-vSwitch-system vRouter-management ip)# exit
sun(config-vSwitch-system vRouter-management)# exit
sun(config-vSwitch-system)# exit
sun(config)#
```

After completing this procedure, return to Step 8 in the procedure, "How to Import Archived Configurations Into a New Switch."

Enhancements

The following describes the enhancements with release V2_0R6. This may include enhancements from other point releases since the 2.0 release.

ACL Route Action

In addition to the existing *permit* and *deny* ACL Rule Action types, the *route* action feature now can route traffic that matches ACL rules to a next hop IP address. This traffic will bypass L4 service classification and be routed to the configured next hop IP address within the same vRouter.

L4 services, which include all virtual service and real service related policy, will be bypassed. When a route action is specified on an ACL rule, a nextHop field is optional. If no nextHop is specified, the frame is routed using the destination IP address in the frame.

This functionality is available only with Release 2.0, Patch 4 (R2_0R4) and later.

To configure to bypass L4 rules between host subnets 10.0.1.0/24 and 11.0.1.0/24, do the following:

```
sun(config-vSwitch-SVS1 vRouter-default)# ip accessList acl10net
enabled
sun(config-vSwitch-SVS1 vRouter-default)# ip accessList acl10net
rule 100 route any ruleSrcAddrs 10.0.1.0/24 ruleDstAddrs 11.0.1.0/
24
sun(config-vSwitch-SVS1 vRouter-default)# ip accessList acl10net
rule 101 permit any
sun(config-vSwitch-SVS1 vRouter-default)# ip accessList acl11net
enabled
```

```
sun(config-vSwitch-SVS1 vRouter-default)# ip accessList acl11net
rule 100 route any ruleSrcAddrs 11.0.1.0/24 ruleDstAddrs 10.0.1.0/
24
sun(config-vSwitch-SVS1 vRouter-default)# ip accessList acl11net
rule 101 permit any
sun(config-vSwitch-SVS1 vRouter-default)# ip accessGroup eth.1.6 in
acl10net
sun(config-vSwitch-SVS1 vRouter-default)# ip accessGroup eth.1.8 in
acl11net
```

Client Address Translation

Address Translation controls whether the client's address will be changed to an address from the Proxy IP Pool for the vRouter that the RealService is using before the packet is sent to the RealService.

The field `clientAddressTranslation` was previously an enable/disable option. This field has been replaced with the `clientAddressTranslationMask` field, which allows you additional flexibility over the previous behavior.

The value of 255.255.255.255, which is the default, disables client address translation and the value of 0.0.0.0 enables client address translation for all clients. Any other value of contiguous 1s and 0s can be used to control the clients that will have their addresses translated.

Supported hardware

The N2000 Series is available in two versions: the N2120 and the N2040. The Sun N2120 platform provides 12 small form-factor pluggable (SFP) Gigabit Ethernet (copper or fiber) ports. The Sun N2040 provides 40 10/100-Mbps ports and 4 small form-factor pluggable (SFP) Gigabit Ethernet (copper or fiber) ports. Both systems are rackmountable and operate on standard AC voltages (115 or 230 VAC) in either redundant or non-redundant power configurations.

Figure 1 illustrates the Sun N2120, and Figure 2 illustrates the Sun N2040.

Figure 1. Sun N2120 Chassis

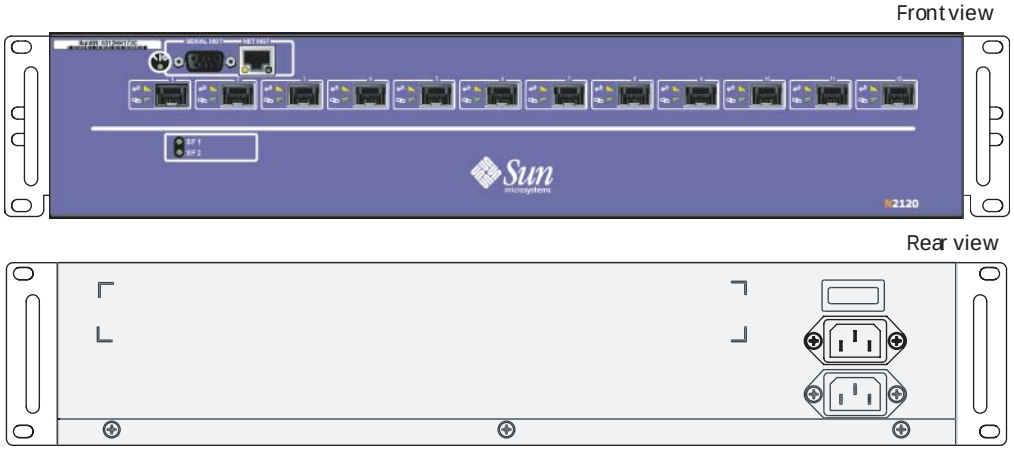
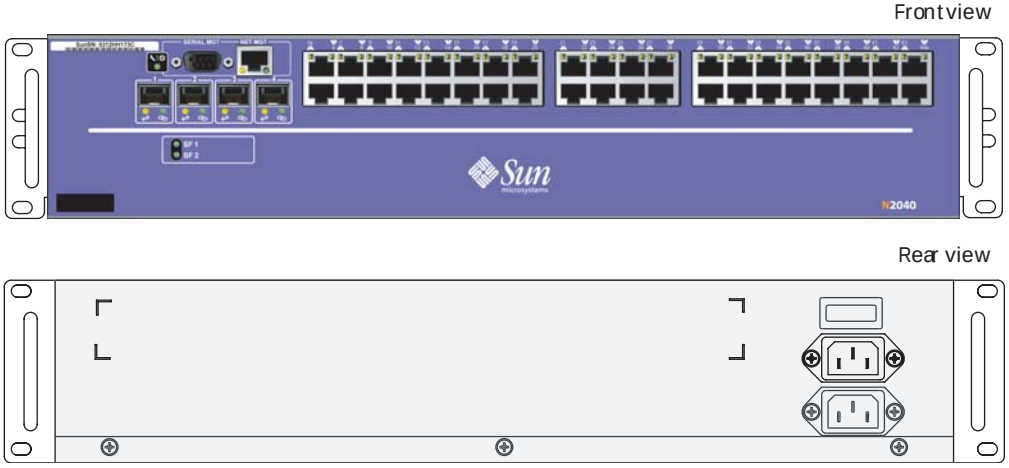


Figure 2. Sun N2040 Chassis



Interface support

Ethernet ports

Ethernet 10/100BASE-T ports require standard UTP/STP network cable, Category 5 or 5E, with RJ-45 8-pin modular connectors.

Gigabit Ethernet ports require SFP LC fiber-optic connectors on multimode fiber-optic cable.

Console and Ethernet management ports

The console port requires a standard EIA-232 (RS-232) data terminal equipment (DTE) crossover serial cable with a DB-9 connector.

The 10/100-Mbps management port requires a standard UTP/STP network cable, Category 5 or 5E, with an RJ-45 8-pin modular connector.

Configure the terminal emulator for a VT100 emulation (or allow autodetection) and then set to 9600 baud, 8 data bits, no parity bit, and 1 stop bit (8/N/1).

Operational considerations

Fiber-optic transceivers

Sun has tested the fiber-optic ports on the front of the system with the following transceivers listed by vendor and vendor part number.

- Picolight PL-XPL-00-S13-05
- Stratos SPLC-20-4-1-B
- Finisar FTRJ-8519-7D

You can use other transceivers, but only the ones listed above have been fully tested. If required, these transceivers can be purchased from Sun or directly from approved vendors.

Software Information

System installation and startup

System startup is performed after you install the chassis into a rack or set it on a flat surface and attach a cable to the system. You must attach a local terminal to the system console port. When ready, turn the system on using the POWER ON/OFF switch on the back of the chassis. A first-time startup takes several minutes.

Refer to the *Sun N2000 Series Release 2.0 – Hardware Installation and Startup Guide* for complete information on performing a system hardware installation.

System configuration file

The system configuration uses the `cdb.dat` file, located on the system disk directory `/ftl0/config`. Refer to the *Sun N2000 Series Release 2.0 – System Administration Guide* for information on managing this file.

Management support

Administrators can use multiple management tools to support the Sun N2000 Series in a network. These tools include:

- Command-line interface
- Web interface
- SNMP

Command-line interface

The command-line interface (CLI) uses an industry-standard design that allows you to configure and manage the N2000 Series by entering keyboard commands. You access the CLI over a direct console connection to the RS-232 port on the front of the system, or over a Telnet or SSH connection. A connection to the CLI is indicated by the user name and password prompts.

Web interface

The Web interface is a graphical user interface that allows you to configure and manage the Sun N2000 Series.

The following operating systems and Web browsers have been tested with Version 2.0.

Operating systems

- Windows 98, 2000, and XP
- Macintosh OS X v 10.1
- Red Hat Linux release 7.1
- Solaris™ 9 4/03

Web browsers

- Microsoft Windows
  - Internet Explorer 5.5 and 6.x
  - Netscape™ 6.2, 7.x
  - Mozilla™ 1.x
  - Firefox 1.0
  - Opera 6.x and 7.x
- Macintosh
  - Internet Explorer 5.2
  - Netscape 6.2
  - Mozilla 1.x
  - Firefox 1.0
- Red Hat Linux
  - Mozilla 1.x
  - Opera 6.x
- Solaris
  - Netscape 7.x

- Mozilla 1.x
- Firefox 1.0

The minimum Macromedia Flash version required is Version 6.0.65.0. Newer versions of Flash (such as 7.x or above) will also work.

The Web interface supports almost all management capabilities provided by the CLI. The Web interface also supports additional functionality, such as graphing, advanced editors, and monitoring tools.

SNMP

The Sun N2000 Series supports the following SNMP versions: SNMP v1, SNMP v2c, and SNMP v3. Sun enterprise MIBs are available on the N2000 Series Documentation CD.

Configuration scaling

Virtualization and management

System vSwitch with:

- Management vRouter
- Four additional vRouters (shared and three additional vRouters)
- With optional virtualization and license key, up to 10 operator-defined vSwitches, each with their own default vRouter
- 100 user accounts (used for login access to the switch)
- 10 concurrent CLI sessions
- 10 concurrent HTTP management sessions

L2 to L3 scale

- Ports per LAG: 16
- LAGs: 22
- Ports or LAGs per VLAN: 44

- VLANs: 4095 per N2000, 512 per vSwitch
- ARP entries per vRouter: 3000
- 4 ACLs per vRouter: 256 rules per ACL
- IP interfaces per vRouter: 128
- Static routes per vRouter: 2000
- MAC entries per system: 16,000

Virtual service configuration

- Maximum number of virtual services per vSwitch: 512
- Service groups per vSwitch: 512
- Real hosts per vSwitch: 1024
- Real services per vSwitch, each able to be health-checked: 1024
- Maximum number of real services in a service group: 1024
- Request policies per vSwitch: 1000
- Response policies per vSwitch: 1000
- Request transforms per vSwitch: 1000
- Response transforms per vSwitch: 1000
- Object rules per vSwitch: 1000
- Configurable health checks per vSwitch, up to one per service group: 512
- Active health checks per vSwitch, up to one per real service: 1024
- Keep-alives per real service (1 probe or 1 list of up to 5 HTTP probes): 1
- 1024-bit certificates per vSwitch, up to one per virtual service: 512

Note: The scaling numbers outlined above are individually achievable, but maximum configurations combining all of the scale factors are not achievable.

Known problems, restrictions, and limitations

This section describes the known problems, restrictions, and limitations in Release 2.0, Patch 06 (V2_0R6). For tracking purposes, an internal Sun reference number is included at the end of each item in this section.

System startup

- After rebooting with a previously saved configuration, a vSwitch's operational status may display as “starting” instead of “UP.” There may also be network processor warnings shown in the syslog, similar to the following:
  `<132> Nov 11 14:38:40 2004 v0 IP.system.shared [0/10167] [WARNING]: vlan.55failed to add IP rule 55.55.55.1 priority 1 to network processor.` (5241)
- When viewing the system vSwitch, the operational status field may display “starting.” This can be ignored. (5788)

CLI

- When exporting a running configuration, you must specify the following parameters in order for the configuration to play back correctly on the switch: `show runningConfig true nameValuePairs true`. (5846)
- When exporting redundant configuration you must edit the output file and remove the certificates used by the HTTPS and SSH management interfaces. (6911)
- When exporting a running configuration you must remove any lines for TCP connections or SSHd sessions. Refer to the Archiving a Version 2.0 Configuration section of this document for more information. (5903)

Web interface

- Most browsers exhibit a security issue regarding the way basic authentication is implemented by continuing to send the old credentials after an error message is received. To avoid this issue, you must close the browser window used to connect to the switch to maintain security and prevent unauthorized access. Mozilla is the only browser that does not exhibit this issue. (1199)
- Online Help requires JavaScript™ enabled on your Web browser. (2104)

- Displaying statistics using line graphs will preserve all history of graphed data, which will continuously consume memory on your PC if left unattended. (2299)

Software Version

The version command is used to switch between various major and minor versions of the software, but not different patch versions. The highest installed patch level for the selected version will be loaded. (5920)

Syslog

- Although most Syslog messages are time-stamped in local time, repeat events are currently time-stamped in GMT time. (5007)
- User may receive the following syslog message: ControlPlane.erp.management [0/10180] [WARNING] : vsa.2.3 connect to ip.5.2 not successful after 2 seconds - still trying. This message is not indicative of a problem and should be ignored. (6372)

SNMP

The SNMP MIBs shipped with this release have some incorrect and omitted descriptions. Refer to the *Sun N2000 Series Release 2.0 – System Configuration Guide* for complete MIB descriptions.

Secure Shell (SSH)

F-Secure SSH client version 5.2 cannot connect with this release. In newer versions of F-Secure, specifically version 5.4, build 32, this issue does not exist. (1349)

FTP

The FTP client on the switch is not accessible through the Web interface. The FTP client must be used within the CLI. (3778)

Ports

- The Ethernet management port will come up as 10/half if set to autonegotiate and connected to an endstation that is not autonegotiating and fixed at 100/full or 100/half. (1211)

- When copper gigabit GBICs are installed, the CLI will display the configuration as fixed 1000M, full-duplex. However, the copper gigabit interface is actually set to autonegotiation, advertising 1000M, full-duplex only. (5686)
- If you import a running configuration file that has port mirroring enabled information will not be properly replayed. The port mirror configuration will have to be manually configured. (5725)
- The default for gigabit ports is hard coded at 1000M, full-duplex for fiber SFPs. The gigabit standard calls for all gigabit ports to be set to autonegotiation. The copper gigabit SFPs do autonegotiate by default. (5812)
- Port mirroring will only mirror traffic received by a port (in), even if it was configured to mirror transmit (out or both) traffic. (5793)
- Auto negotiation does not work using the NS-83820 Fiber NIC and the Finisar SFF optical GBIC (part number FTRJ-8519-3). The SFF optical GBIC PicoLight, (part numbers: PL-XPL-00-S13-05 & PL-XPL-S23-28) will auto negotiate with the NS-83820 Fiber NIC. (5682)

Jumbo frames

Jumbo frames directed to the switch IP address are dropped. (1665)

IP routing

- Directed broadcasts are not forwarded across IP interfaces. (2059)
- The on-board `traceroute` command fails in an on-board IP interface. The ICMP `ping` command can be used. (5092)

ICMP

The switch does not always properly respond to ICMP Address Mask requests properly. (3946)

OSPF

OSPF type 2 AS external routes always use a metric of 1 regardless of the configured metric. (5693)

Access control lists (ACLs)

- ACLs will not block traffic that is generated internally within the N2000 Series application, such as RIP advertisements, outgoing Spanning Tree BPDUs, etc. (2225)
- The number of ACLs that can be applied to interfaces across the switch will vary with the complexity of the rules that are applied. If the internal table limits are exceeded, an error will be generated and reported through the syslog facility.
- When creating ACLs, you must create all the rules in the `accessList` before adding it to an `accessGroup`. You must also remove `accessList` from and `accessGroup` before modifying any of the rules. If you do not follow this process, the ACL will not function properly. (5821)

Routing Information Protocol (RIP)

The switch will erroneously add a host route to the route table based on a received RIP update when the switch has already received a RIP update containing a route with a short mask for the same gateway. This compliance problem should have no negative network impact. (2457)

Statistics

- IP statistics will occasionally show up as N/A when an IP interface is being flooded with bad packets. (3666)
- Spanning Tree Protocol BPDUs are not counted in VLAN interface statistics. (1055)
- The IP Stat “Out No Route” is incremented during Static NAT. Static NAT traffic flow from server side to client/Internet side results in “Out No Route” in the IP stats for the vrouter.

VSRP

When you delete a VSRP Node configuration, the VSRP Node and peer configuration are both deleted, but the session configuration is not deleted. (6277)

Load balancing

- Opera Web browsers continue to request TCP data even when receiving a TCP-RST. This can cause the browser to appear hung. (2844)
- UDP load balancing (including RADIUS and DNS) does not support frames with IP options. (4469)
- UDP services (TFTP and NFS) do not work in a Dynamic NAT configuration. These services must be configured static NAT only. (5611)
- With request and response transforms, only defined headers can be used in the "Delete HTTP Header" field. The list of defined headers can be found in the *Sun N2000 Series Release 2.0 – System Configuration Guide*. If a non-defined header is used, compilation warnings will be triggered and the virtual service will show an "Oper Message" of "Object rule compilation error." (5800)
- Posts with content-length greater than 20k will not be retried to `realServices` and may require the user to resubmit the post. (6296)
- User can create a Static NAT entry that conflicts with the VRRP assigned address. N2000 does not parse for duplicated IP addresses for the Static NAT ranges compared to the VRRP definitions. (6297)
- When you create Static NAT entries in separate vSwitches, the second entry is not fully configured. (6304)
- Connection Failures with Persistent HTTP/1.1 and `srcAddress sticky` enabled. (6308)
- If you create more than 128 PIP addresses on a single vSwitch or more than 512 PIP addresses on the switch, there is a potential for routing instability. Limit the number of PIP addresses so as to not exceed these values. (6113)

Documentation updates

This section describes updates in the Sun N2000 Series documentation. Refer to the following Sun Web site for the most recent versions of documentation for this product.

`http://www.sun.com/products/networking/switches`

The official product name is the Sun Secure Application Switch - N2000 Series. Throughout the documentation, the product is referred to as the “N2000 Series,” the “Sun Application Switch,” the “application switch,” the “switch,” or the “system.”

Manuals

With this release, all documents have been updated to reflect the new functionality.

- Throughout the documentation set, whenever the `show runningConfig` or the `show redundantConfig` command is shown with examples of CLI output, the underscore (_) precedes the CLI output. That underscore no longer exists in the current version of the software.
- Throughout the documentation set and in each particular book, there is a Regulatory Compliance Statement, which includes a CCC Class A Notice applicable to products shipped to China. Disregard this notice in the documentation, since the CCC Class A Notice is not applicable to this product. This notice should not be in this documentation and will be removed for the next release of the product documentation.
- In all versions of the Introduction Guide, there is no description of the Feedback button that exists in the Web interface. This button description should be located in the Introduction Guide, in the “Additional Help features” section within the Help section of Chapter 2. When you click the Feedback button, you are brought to a Sun Documentation Feedback Web page.

Quick Installation

- In Step 2, the text states that you can “Install the chassis into a 4-post rack.” The text should also state that you can install the chassis into a 2-post rack as well.

Command Reference

- When tabular output is produced by a CLI `show` command, a dashed line separates the table headings from the data. The dashed line is not shown in the examples in the *Sun N2000 Series Release 2.0 – Command Reference*.
- All instances of the `show redundant-config` command within the book should say `show redundantConfig`.
- All instances of the `show running-config` command within the book should say `show runningConfig`.

- In the `loadBalance realService` command, the `clientAddressTranslation` field has been replaced with the `clientAddressTranslationMask` field. Refer to the section, Client Address Translation, for additional information.
- On page 12-3, the software key example currently shows the example as `01-0000-62399fa71d16833fc49a`. The correct software key output example is `01-0000-6239-9fa7-1d16-833f-c49a`.
- On page 16-1, the book currently states that you can create a total of 5 shared vRouters (a system-created/shared vRouter and four additional ones). You only can create a total of 4 shared vRouters (a system-created/shared vRouter and three shared ones).
- On page 29-243, in the Output Description table and within the `Peak Active Sessions` field name description, the second sentence currently states, “This count includes sessions in the TIME_WAIT state, ...” That sentence should actually state, “This count does not include sessions in the TIME_WAIT state, ...”

System Configuration Guide

- All instances of the `show redundant-config` command within the book should say `show redundantConfig`.
- All instances of the `show running-config` command within the book should say `show runningConfig`.
- In the `loadBalance realService` command, the `clientAddressTranslation` field has been replaced with the `clientAddressTranslationMask` field. Refer to the section, Client Address Translation, for additional information.

System Administration Guide

- On page 12-3, the section under “Changing software versions” entitled “CLI Session - change to a different software version” is incorrect and does not include the correct examples in the command example. Currently, you also cannot switch between different patch versions of this release.

Online Help

- Opera 7.x (in Solaris™ and Windows environments) does not display Help correctly or support correct navigation between topics.
- The Table of Contents in the Web interface does not expand or collapse if you are using any of the Opera 6.x point releases. If you need to use the Table of Contents for the Help, you must use either Opera 7 or the supported versions of Mozilla and Internet Explorer. The context-sensitive Help and Help indexes work properly in Opera 6.x point releases.