

NetApp[®] 1G Cluster-Mode Switch Installation Guide

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089 U.S.A.
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: www.netapp.com

Part number: 215-06285_B0
July 2013

Copyright and trademark information

Copyright information

Copyright © 1994-2013 NetApp, Inc. All rights reserved. Printed in the U.S.A.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, FAServer, FilerView, FlexCache, FlexClone, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), ONTAPI, OpenKey, RAID-DP, ReplicatorX, SANscreen, SecureAdmin, SecureShare, Select, Shadow Tape, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMirror, SnapMover, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, and Web Filer are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks. NetApp, Inc. NetCache is certified RealSystem compatible.

Table of Contents

Chapter 1	NetApp CN1601 Switch Features	5
	Hardware components	6
	Software features	10
	Technical specifications	16
 Chapter 2	 Hardware Installation.	 19
	Before you begin	20
	Installing the switch	22
	Connecting to ports and power	26
 Chapter 3	 Switch Management.	 29
	Accessing the management interface.	30
	Boot process	35
	Startup Utility functions	38
	 Glossary	 41
	 Index	 45

About this guide

Purpose and audience

This guide provides an overview of the NetApp® CN1601 switch hardware and software features and describes the procedures to install the switch and to access the command-line interface (CLI). This document is intended for network administrators responsible for installing and managing network equipment.

Terms and acronyms

In most cases, acronyms are defined on first use.

Various technical terms and acronyms in this document are also defined in “[Glossary](#)” on page 41.

Document conventions

The following conventions may be used in this document:

Convention	Description	Example
courier font	Command or command-line text	show vlan brief
<i>italic courier font</i>	Variable value. Replace the italicized text with an appropriate value, which might be a name or number.	show vlan <i>vlan_id</i>
[] square brackets	Optional parameter.	[value]

Additional documentation

The following documentation provides additional information about the CN1601:

- ◆ The *NetApp CN1601 Network Switch CLI Command Reference* describes the commands available from the command-line interface (CLI) for managing, monitoring, and configuring the switch.
- ◆ The *NetApp CN1601 Network Switch Administrator's Guide* contains step-by-step configuration examples for several features.

About this chapter	This chapter describes the CN1601 switch hardware components and software features and provides technical specifications.
Topics in this chapter	<p>This chapter includes the following topics:</p> <ul style="list-style-type: none">◆ “Hardware components” on page 6◆ “Software features” on page 10◆ “Technical specifications” on page 16
CN1601 summary	<p>The CN1601 is a managed Layer 2 switch that provides 16 10/100/1000Base-T ports.</p> <p>This 1U switch can be installed in a standard 19-inch NetApp 42U system cabinet or third-party cabinet.</p> <p>The switch supports local management through the console port or remote management by using Telnet or SSH through a network connection. You can manage the switch by entering commands into the command-line interface (CLI) or by using an SNMP-based network management system (NMS).</p>

Hardware components

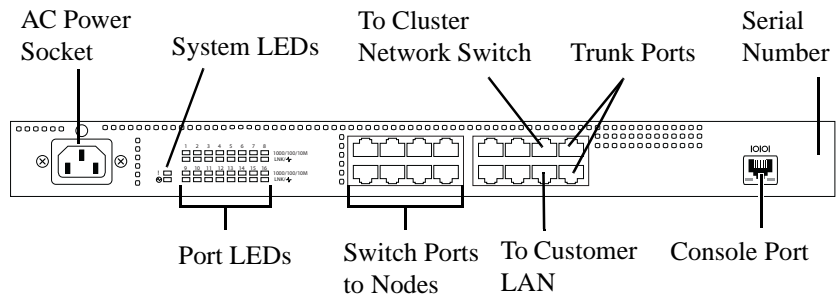
Physical description

The CN1601 has a 1U chassis design and is rack-mountable in a standard 19-inch equipment rack or a NetApp 42U System Cabinet.

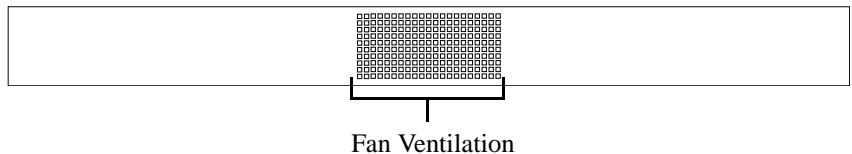
The rear panel of the switch provides the following components:

- ◆ Switch ports that connect to:
 - ❖ Nodes
 - ❖ Other switches (trunk ports)
 - ❖ Cluster network switch
 - ❖ Customer LAN
- ◆ Console port
- ◆ AC power socket
- ◆ System and port LEDs

The following figure shows the rear panel of the switch:



The front panel provides ventilation for the system fans:



Gigabit Ethernet ports

The switch has 16 gigabit Ethernet (10/100/1000Base-T) RJ-45 ports that support the following features:

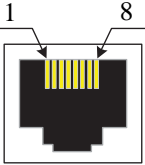
- ◆ Auto-MDIX to automatically detect the difference between crossed and straight-through cables.
- ◆ Half- and full-duplex mode.
- ◆ Auto-negotiation to automatically detect the speed and duplex mode of the connected device.

Console port

The console (RJ45) port is used only for management through a serial interface. This port provides a direct connection to the switch and allows you to access the CLI from a console terminal connected to the port through the provided serial cable (RJ45 to female DB-9 connectors).

The console port supports asynchronous data of eight data bits, one stop bit, no parity bit, and no flow control. The default baud rate is 9600 bps.

The pin assignment for the console port is shown in the following table:

Connector	Pin Number	Signal
	1	Not used
	2	Not used
	3	Transmit data (TDX)
	4	Signal ground (GND)
	5	Signal ground (GND)
	6	Receive Data (RXD)
	7	Not used
	8	Not used

Port LED definitions Each switch port has two LEDs that provide port link/activity and speed information.

The port LEDs are between the power socket and the switch ports. Each pair of LEDs is labeled with the port number the LEDs represent. The Speed LED is on top, and the Link/Activity LED is directly below it.

The following table describes the Speed and Link/Activity LEDs associated with ports 1 through 16:

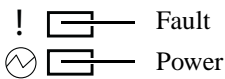
RJ-45 port LED	Color	Description
Speed	Green	A valid 1000 Mbps link is established on the port.
	Amber	A valid 100 Mbps link is established on the port.
	Off	The link is operating at 10 Mbps, or no link is present.
Link/Activity	Solid green	A valid link is established on the port.
	Blinking green	The port is transmitting or receiving packets.
	Off	No link is established on the port.

Fan and power supply information The CN1601 includes one internal 40-watt AC power supply that powers the switch when connected to an AC power source.



Two fans are located in the switch directly behind the front panel. The airflow direction is front-to-back.

System LED definitions

The system LEDs provide information about the overall system status. The following figure identifies the two system LEDs:



The following table describes the system LEDs:

System LEDs	Color	Description
 Fault	Yellow	The switch has experienced a failed condition.
	Off	The switch is operating normally.
 Power	Green	The power supply is operating normally.
	Off	The switch does not have power.

Software features

Operating system features

The switch operating system features include those that allow you to define the switch within your network and manage or monitor various hardware and software aspects.

The following table describes the system features:

System feature	Description
Remote management	Remote management of the switch over the in-band network is available by using any of the following protocols: <ul style="list-style-type: none">◆ Telnet◆ SSH v1.5, v2◆ TFTP◆ SNMP v1/v2c/v3
BootP/DHCP client	Automatically obtain network information, such as an IP address for the management interface, from a BootP or DHCP server on the network.
SNTP client	Synchronize the time on the switch with a remote SNTP server. The switch supports SNTP Version 4.
DNS client	Specify the DNS server to use to resolve host names to IP addresses.
Dual image support	Store up to two software images and two configuration files on the switch flash file system. This allows you to upgrade the switch software while leaving the possibility of reverting to the old software or old configuration.
File download and upload	Download files such as firmware images and configuration files to the switch by using TFTP, SCP, SFTP, and XMODEM. Files can also be uploaded from the switch to a remote system.

System feature	Description
CLI scripting	Download a text file containing CLI commands to the switch and execute all commands in order. The script can be modified and downloaded to multiple switches.
IPv6 management	<p>The switch supports the following IPv6 management protocols and applications:</p> <ul style="list-style-type: none"> ◆ Pingv6 ◆ Traceroutev6 ◆ TFTP ◆ SSH ◆ SSL ◆ TELNET ◆ SNMP
Logging	Maintain a record locally on the switch or on a remote Syslog server of switch events, including CLI commands executed on the switch. Control the severity of messages to log.
System monitoring	View information about the system temperature, power supply, and fan status.
Remote monitoring (RMON)	<p>The switch supports the following four groups defined as part of the RMON standard:</p> <ul style="list-style-type: none"> ◆ Statistics ◆ History ◆ Alarms ◆ Events

Switching features

The switching features include the Layer 2 features described in the following table:

Switching feature	Description
Port control	Configure individual port settings such as administrative status, speed, duplex, and autonegotiation mode.
Layer 2 forwarding database (L2FDB) control	Add static addresses or clear the L2FDB and control the number of entries that can be dynamically learned.
Layer 2 multicast forwarding database (MFDB) control	Limit multicasts to only certain ports in the switch to prevent traffic from going to parts of the network where that traffic is unnecessary.
VLANs	Optimize network traffic patterns by creating VLANs and configuring member ports so that broadcast, multicast, and unknown unicast packets are sent only to ports that are members of the VLAN.
Protocol-based VLANs	Define a packet filter that the switch uses as the matching criteria to determine if a particular packet belongs to a particular VLAN. With protocol-based VLANs, traffic is bridged through specified ports based on its protocol.
MAC-based VLANs	Assign incoming packets to VLANs based on the source MAC address of the packet.
IP subnet-based VLANs	Assign incoming packets to VLANs based on the source IP address of the packet.
Double-VLAN tagging	Allow the use of a second VLAN tag on network traffic to help differentiate between customers in the Metropolitan Area Networks (MANs) while preserving individual customer's VLAN identification when they enter their own 802.1Q domain.

Switching feature	Description
Link Layer Discovery Protocol (LLDP) - IEEE802.1AB	Permit stations residing on an 802 LAN to advertise major capabilities and physical descriptions allowing a network management system (NMS) to access and display this information.
Industry Standard Discovery Protocol (ISDP)	Discover and share information between the switch and neighboring devices (routers, bridges, access servers, and switches). ISDP interoperates with Cisco® network equipment that uses CDP.
IEEE 802.1AX link aggregation	Increase bandwidth between two switches by aggregating multiple ports in one logical Link Aggregation Group (LAG), which is also known as a port channel. The switch treats the LAG as if it were a single link. The switch supports both static and dynamic LAGs.
IEEE 802.1s Multiple Spanning Tree (MSTP)	Prevent and resolve L2 forwarding loops by using MSTP to map VLANs to spanning tree instances.
IGMP snooping	Allow the switch to snoop IGMP packets to limit the number of ports that forward multicast traffic. This allows the switch to conserve bandwidth on those segments of the network where no node has expressed interest in receiving packets addressed to the group address.
Port mirroring	Copy the traffic from multiple source ports to a single destination port. The primary use of this is to analyze switch traffic by using a network analyzer on the destination port.
Flow-based mirroring	Copy certain types of traffic to a single destination port. You can configure the switch to mirror flows based on Layer 2, Layer 3, and Layer 4 information.
Storm control	Protect the network by detecting a traffic storm (broadcast, multicast, or unknown unicast traffic received at a very high rate) and preventing these packets from flooding other parts of the network.

Quality of Service (QoS) features

QoS features affect the way traffic is handled as it enters and exits the switch. The following table describes the QoS features:

QoS Feature	Description
IP Access Control Lists (ACLs)	Create one or more rules that cause traffic to be forwarded, dropped, or assigned to a specific queue based on the match criteria within the IP packet.
MAC ACLs	Create one or more rules that cause traffic to be forwarded, dropped, or assigned to a specific queue based on the match criteria within the Ethernet frame.

Security features

The security features include settings that protect against unauthorized and unauthenticated access to the switch management interface as well as settings that protect against unauthorized and unauthenticated access to the network through the switch ports. The following table describes the security features:

Security feature	Description
User management	Configure the username and password for users allowed to access the switch management interface.
Authentication list	Specify the authentication method for different access types.
Denial of Service (DoS) protection	Provide protection against DoS attacks on the switch and on the network.
IEEE 802.1X port-based access control	Prevent unauthorized devices from accessing the network through the switch on a per-port basis.
RADIUS client	Allow the switch to communicate with a network RADIUS server to authenticate users prior to access to the switch management or to the network.

Security feature	Description
TACACS+ client	Allow the switch to communicate with a network TACACS+ server to authenticate users prior to access to the switch management or to the network.
Management ACL	Ensure that users' remote connections to the switch management interface are through known and trusted devices.

Technical specifications

Physical characteristics

The following table lists the physical characteristics of the CN1601 switch:

Specification	Measurement
Height	43 mm (1.69 in)
Width	445 mm (17.5 in)
Depth	508 mm (20 in)
Weight	5.45 kg (12 lbs)

Network protocol and standards compatibility

The CN1601 switch supports the following network protocols and standards:

- ◆ IEEE 802.3i 10Base-T
- ◆ IEEE 802.3u 100Base-TX
- ◆ IEEE 802.3x Flow-Control
- ◆ IEEE 802.3ab 1000Base-T

Environmental specification

The following table lists the environmental specification for the CN1601 switch:

Specification	Measurement
Operating temperature:	10 to 40°C
Storage temperature	-40 to 70°C
Operating relative humidity	20 to 80% noncondensing
Storage relative humidity	10 to 95% noncondensing

Power specifications

The following table lists the power specifications for the CN1601 switch:

Specification	Measurement
AC-input frequency (universal)	50 to 60 Hz
AC-input voltage (universal)	100 to 240 VAC
Power supply	40W
DC-output voltage	12V

About this chapter

This chapter contains information about preparing to install the CN1601 hardware and provides step-by-step instructions about installing and powering on the switch.

Topics in this chapter

This chapter includes the following topics:

- ◆ [“Before you begin”](#) on page 20
- ◆ [“Installing the switch”](#) on page 22
- ◆ [“Connecting to ports and power”](#) on page 26

Before you begin

Site preparation

The location and conditions of the place where you decide to install the CN1601 must conform to the following guidelines:

- ◆ The location must be clean, dry, and well ventilated.
- ◆ The location must meet the specifications described in “[Environmental specification](#)” on page 16.
- ◆ The installation site must have sufficient space to allow access to the front and back panels of the switch.
- ◆ The system and port LEDs must be visible.
- ◆ The power cord must be able to reach from the power socket on the switch to a properly-grounded power source.
- ◆ The cable length from the copper Ethernet ports to the connected devices must not exceed 328 feet (100 meters).
- ◆ The ventilation holes on the front and rear panels must not be obstructed in order to provide proper airflow through the switch.
- ◆ The cabling must be routed away from sources of electrical interference such as power lines and fluorescent lighting fixtures.

Verify package contents

The CN1601 package includes the following contents:

- ◆ NetApp CN1601 switch
- ◆ Software license and warranty information
- ◆ Rack-mount installation kit
- ◆ RJ45 to DB-9 console cable

Power cables are a separate item and not included in this package. If any item is missing or damaged, contact your authorized NetApp sales representative immediately.

Required tools and equipment

Before installing the switch in a standard equipment rack or NetApp 42U System Cabinet, make sure you have the following equipment:

- ◆ Number 2 Phillips screwdriver
- ◆ Two standard rack screws
- ◆ Electrostatic discharge (ESD) wrist strap
- ◆ Cage nut installation tool

Installing the switch

Rack-mounting the switch

The mounting brackets are preinstalled on the front panel of the switch chassis. Use the following procedures to install the switch in a standard 19-inch NetApp 42U system cabinet or third-party cabinet.

Note

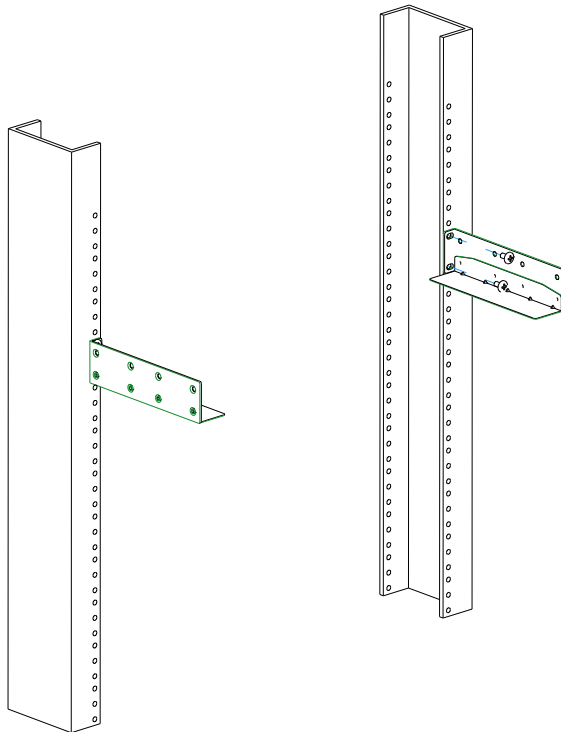
The CN1601 switch cannot be mounted flush with the U markers on the rear side of the cabinet/rack.

Note

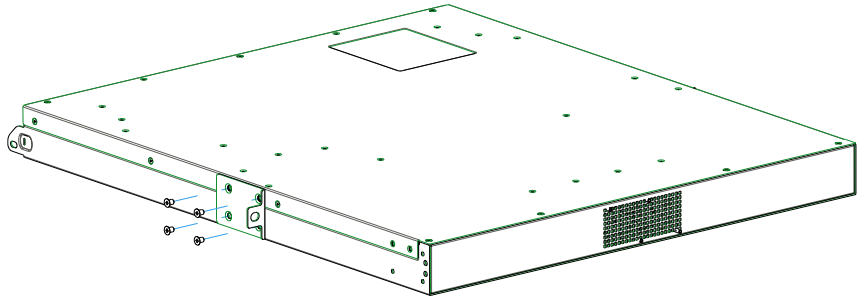
The preferable mounting position is in the far back position of the rack when equipment above or below the switch is deeper in detention.

To install the switch in a two-post rack:

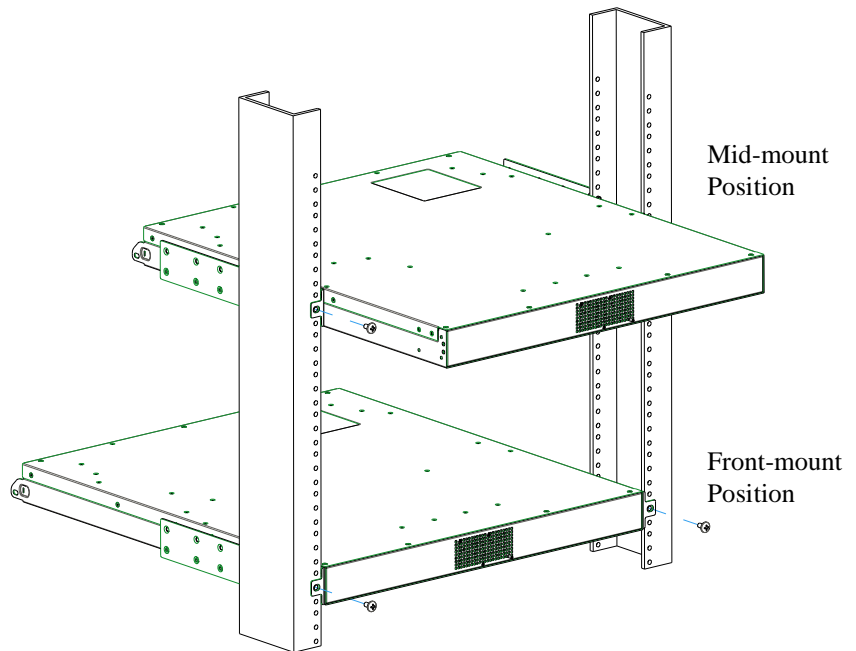
1. Using rack screws, install the support rails into a two-post rack.



2. If necessary, relocate the chassis mounting ears from the front-mounting position to the mid-mount position.

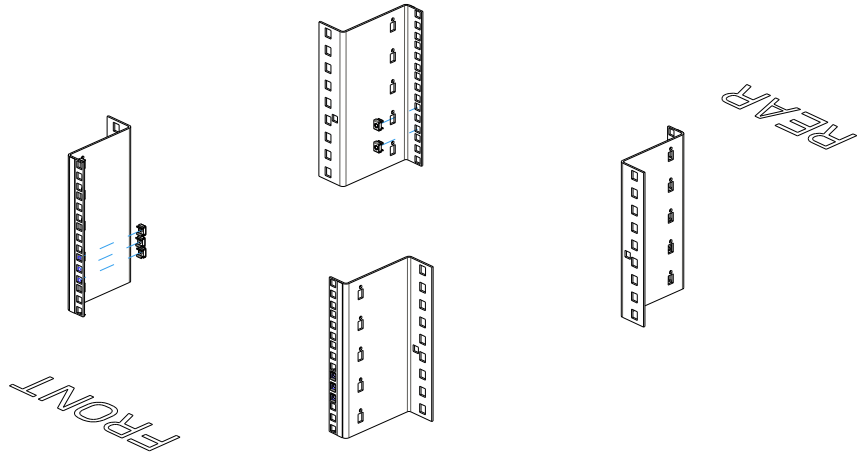


3. Install the chassis on the support rails and secure the chassis mounting ears to each rack post by using screws.

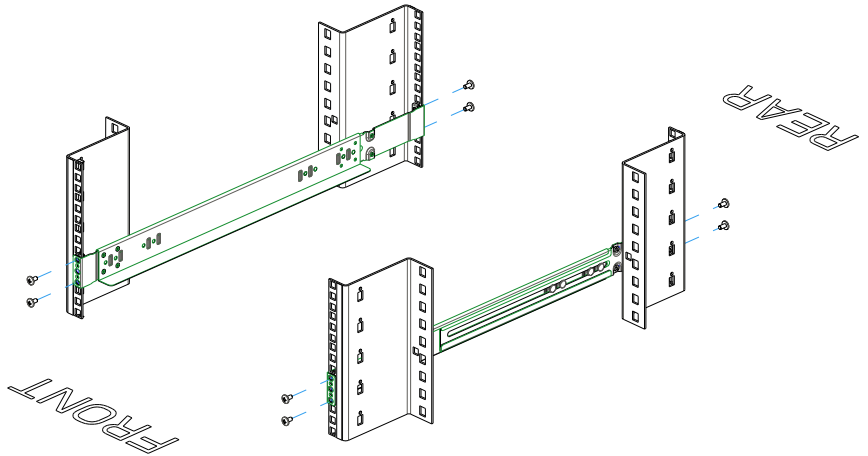


To install the switch in a four-post rack:

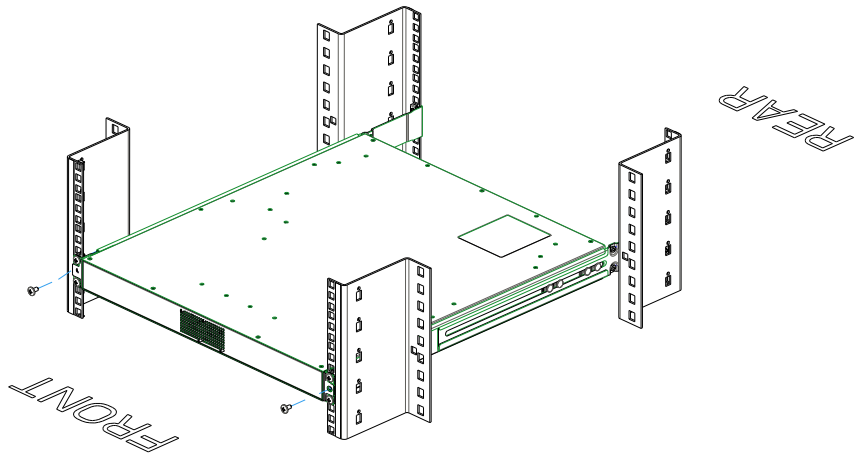
1. Install three clip-nuts to the front rack and two to the rear rack. Apply the clip nuts to both the left and the right racks.



2. Use screws to install the support rails to the four-post racks.



3. Install the chassis on the support rails and secure the chassis to the front rack by using screws.



Connecting to ports and power

Connecting to the 10/100/1000BASE-T Ethernet ports

Use Category 5 (Cat5) Unshielded Twisted-Pair (UTP) cable terminated with an RJ-45 connector to connect devices to the 10/100/1000BASE-T Ethernet ports. You can also use Cat6 cables to connect to the Ethernet ports.

The auto-MDIX feature is enabled by default, so it does not matter whether you use a straight-through or crossover cable to connect a device to the switch. With auto-MDIX enabled, the switch detects whether a crossover or straight-through cable connection type is required and automatically configures the port for the appropriate connection.

Note

The cable length between the switch and the attached device is limited to 100m (328 ft.).

When a link is established between the switch and the connected device, the link LED is green.

Connecting power to the switch

The CN1601 switch does not have an ON/OFF switch. Power to the switch is controlled by the power cord connection.

Make sure the AC outlet you select is grounded, can be accessed quickly and easily, and is not controlled by a wall switch that someone might accidentally turn off.

After selecting an appropriate outlet, follow these steps to apply AC power to the switch:

1. Connect the end of the power cable to the power receptacle on the rear panel of the switch.
2. Connect the power cord to the power source.
3. Verify that the Power LED on the switch rear panel is green.

Connecting to the console port

The console port uses an RJ45 connector for serial communication to the switch. The supplied serial cable has an RJ45 connector on one end and a DB-9 connector on the other end. To make the console connection, insert the RJ45 connector into the console port on the switch, and attach the DB-9 connector to the serial (COM) port on a VT100/ANSI terminal or a workstation.

For console port pinout information, see “[Console port](#)” on page 7.

For information about accessing the CLI by using the console port, see “[Connecting to the CLI by using the console port](#)” on page 31.

About this chapter

After you install and power on the switch, the switch boots and becomes operational. This chapter provides information about accessing the switch command-line interface and performing boot-menu functions.

For information about configuring switch features, see the *CN1601 Network Switch CLI Command Reference* and the *CN1601 Network Switch Administrator's Guide*.

Topics in this chapter

This chapter includes the following topics:

- ◆ [“Accessing the management interface”](#) on page 30
- ◆ [“Boot process”](#) on page 35
- ◆ [“Startup Utility functions”](#) on page 38

Accessing the management interface

Local and remote management

Local access to the switch command-line interface (CLI) is available through the console port on the rear panel of the switch. To view the CLI and execute commands from the local connection, use a VT100/ANSI terminal or an administrative computer with terminal emulation software such as Tera Term, xterm, or Windows® HyperTerminal.

To enable remote management of the switch through Telnet, SSH, or SNMP, the switch must be connected to the network and must have an IP address or IPv6 address. After the switch is physically and logically connected to the network, you can manage and monitor the switch remotely by using a Telnet or SSH client (such as PuTTY) on an administrative computer, or by using an SNMP-based network management system. You can also continue to manage the switch through the terminal interface by using the console port connection.

Configuring network information

Management of the switch by using Telnet, SSH, or SNMP requires that the switch be configured with basic network information, including an IP or IPv6 address. The switch has no IP address by default, and DHCP is disabled by default. For more information on configuring the network see the *NetApp CN1601 and CN1610 Setup and Configuration Guide*.

After you perform the physical hardware installation, you need to make a serial connection to the switch so that you can perform one of the following tasks:

- ◆ Manually configure static network information for the management interface, or
- ◆ Enable the management interface as a DHCP or BootP client on your network and then view network information that has been dynamically assigned by the DHCP server on your network.

Connecting to the CLI by using the console port

To access the CLI by using the console port, follow these steps:

1. Using the supplied RJ45 to DB-9 console cable, connect a VT100/ANSI terminal or a workstation to the console (serial) port.

If you attached a PC, Apple®, or UNIX® workstation, start a terminal-emulation program, such as HyperTerminal, xterm, or Tera Term.

2. Configure the terminal-emulation program to use the following settings:

- ❖ Baud rate: 9600 bps
- ❖ Data bits: 8
- ❖ Parity: none
- ❖ Stop bit: 1
- ❖ Flow control: none

3. If the switch is off, power on the switch.

If you are connected to the switch through the console port during the boot process, you can view information that displays during the boot process and access the boot menu. For information about the boot process, including how to access the boot menu, see “[Boot process](#)” on page 35.

4. When the switch has completed the boot process and is operational, press Enter, and the `User:` prompt appears.

Enter `admin` as the user name. There is no default password. Press Enter at the password prompt if you did not change the default password. For information on how to change the password, see the *NetApp CN1601 and CN1610 Setup and Configuration Guide*.

After a successful login, the screen shows the system prompt, for example `(CN1601) >`.

5. At the `(CN1601) >` prompt, enter `enable` to enter the Privileged EXEC command mode.

There is no default password to enter Privileged EXEC mode. Press Enter at the password prompt if you did not change the default password.

The command prompt changes to `(CN1601) #`.

For information about the command modes, see the *CN1601 Network Switch CLI Command Reference*.

Enabling the DHCP or BootP client

Before you can connect to the switch by using Telnet, SSH, or SNMP, the switch must obtain an IP address, subnet mask, and default gateway.

To configure the switch to obtain network information from a DHCP or BOOTP server on the network, follow these steps:

1. Access the switch CLI by using the console port and enter Privileged EXEC mode as described in [“Connecting to the CLI by using the console port”](#) on page 31.
2. Enable the DHCP or BOOTP client on the switch:
 - ❖ To enable DHCP, enter the following command from Privileged EXEC mode:
`network protocol dhcp`
If the command is not available, make sure you are in Privileged EXEC mode. In Privileged EXEC mode, the switch hostname is in parentheses followed by a pound symbol, for example (switch) #.
 - ❖ To enable BootP, enter the following command from Privileged EXEC mode:
`network protocol bootp`
3. Optionally, to enable the DHCPv6 client on the switch, enter the following command:
`network ipv6 address dhcp`
4. Enter the `show network` command to view the network information assigned to the switch by the network server:

```
(CN1601) #show network
Interface Status..... Up
IP Address..... 192.168.10.103
Subnet Mask..... 255.255.255.0
Default Gateway..... 192.168.10.1
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is ..... fe80::210:18ff:fe82:1993/64
Burned In MAC Address..... 00:10:18:82:19:93
Locally Administered MAC address... 00:00:00:00:00:00
MAC Address Type..... Burned In
Configured IPv4 Protocol..... DHCP
Configured IPv6 Protocol..... DHCP
```

```
DHCPv6 Client DUID..... 00:03:00:06:00:10:18:82:19:93
IPv6 AutoConfig Mode..... Disabled
Management VLAN ID..... 1
```

5. Optionally, to save the current configuration so all changes are retained during a switch reset, enter:

```
write memory
```

Configuring static network information

To manually configure a static IPv4 address, subnet mask, and default gateway on the management interface, follow these steps:

1. Access the switch CLI by using the console port and enter Privileged EXEC mode as described in “[Connecting to the CLI by using the console port](#)” on page 31.
2. Optionally, to clear any existing IP address information and set the address configuration mode to static, enter:

```
network parms none
network protocol none
```

3. To configure the static IP address, subnet mask, and default gateway, enter the following command:

```
network parms ip-address netmask [gateway]
```

For example, to configure the management interface with an IP address of 192.168.2.23, a subnet mask of 255.255.255.0, and a default gateway of 192.168.2.1, enter the following command:

```
network parms 192.168.2.23 255.255.255.0 192.168.2.1
```

4. Optionally, to manually configure the IPv6 address, prefix, and default gateway, enter the following commands:

```
network ipv6 address ipv6-address/prefix-length [eui64]
network ipv6 gateway gateway
```

For example, to configure the management interface with an IPv6 address/prefix of 2001:DB8:132::3/32 and a default gateway of 2001:DB8:132::1/32, enter the following commands:

```
network ipv6 address 2001:DB8:132::3/32
network ipv6 gateway 2001:DB8:132::1
```

5. To verify the configured information, enter the following command:

```
(CN1601) #show network
Interface Status..... Up
IP Address..... 192.168.2.23
Subnet Mask..... 255.255.255.0
Default Gateway..... 192.168.2.1
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is ..... fe80::210:18ff:fe82:64c/64
IPv6 Prefix is ..... 2001:DB8:132::3/32
IPv6 Default Router is ..... 2001:DB8:132::1
Burned In MAC Address..... 00:10:18:82:06:4C
Locally Administered MAC address.... 00:00:00:00:00:00
MAC Address Type..... Burned In
Configured IPv4 Protocol ..... None
Configured IPv6 Protocol ..... None
DHCPv6 Client DUID ..... 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode..... Disabled
Management VLAN ID..... 1
```

6. Optionally, to save the current configuration so all changes are retained during a switch reset, enter:

```
write memory
```

Boot process

Booting the switch

To boot the switch, connect a power cord from an AC power source to a power socket on the switch rear panel. If the switch is already powered up, you can enter the `reload` command from the CLI to reboot the switch.

If you are connected to the console port when you power on the switch, you can view system messages that print to the screen during the boot process.

Accessing the Startup Utility menu

After the first part of the boot process is completed, you can invoke the Startup Utility menu and use one or more available menu options, if necessary, to run special procedures. For information about the options available from the boot menu, see “[Startup Utility functions](#)” on page 38.

To boot the switch and access the Startup Utility menu, follow these steps:

1. Connect to the switch through the console port and set the terminal settings appropriately as described in “[Connecting to the CLI by using the console port](#)” on page 31.
2. Start the boot process by using one of the following methods:
 - ❖ If the switch is powered on and operational, reset the switch by entering the following command from Privileged EXEC mode:
`reload`
 - ❖ If the switch is powered off, connect the power supply to the switch.

As the switch boots, the bootup test first counts the switch memory availability and then continues to boot.

3. Watch the screen until the following message appears:

```
FASTPATH Startup Rev: 6.3
```

```
Select startup mode. If no selection is made within 5
seconds,the FASTPATH Application will start automatically...
```

```
FASTPATH Startup -- Main Menu
```

- 1 - Start FASTPATH Application
- 2 - Display Utility Menu

```
Select (1, 2): 2
```

4. To access the Startup Utility menu, press 2 within the first five seconds after the Main menu message appears.

If you do not press 2 within five seconds, or if you press 1, the operational code continues to load. To restart the boot process to access the Startup Utility menu, wait until the switch has completed the boot cycle to reload the switch.

After you press 2, the Startup Utility menu appears:

```
FASTPATH Startup -- Utility Menu
```

- 1 - Start FASTPATH Application
- 2 - Erase Current Configuration
- 3 - Erase Permanent Storage
- 4 - Activate Backup Image
- 5 - Start Diagnostic Application
- 6 - Reboot

```
Q - Quit from FASTPATH Startup
```

For information about the options available from the menu, see “[Startup Utility functions](#)” on page 38.

Next steps

At the end of the boot process, the switch loads the saved configuration. When the process has successfully completed, the `User:` login prompt appears. To enter User EXEC mode, enter `admin`, which is the default user, and press Enter at the password prompt. The `admin` user does not have a password by default. The User EXEC mode offers a limited set of commands. To enter Privileged EXEC mode, enter the `enable` command from User EXEC mode. At the password prompt, press Enter. By default, no enable password is configured.

From Privileged EXEC mode, you can execute all `show` commands to view information about the switch configuration. You can also enter the `configuration` command to enter Global Configuration mode to configure a variety of switch features.

For information about configuring switch features, see the *CN1601 Network Switch CLI Command Reference* and the *CN1601 Network Switch Administrator's Guide*.

Startup Utility functions

Start FASTPATH Application

Use option 1 to resume loading the operational code. After you enter 1, the switch exits the Startup Utility menu and the switch continues the boot process.

Erase Current Configuration

Use option 2 to clear changes to the startup-config file and reset the system to its factory default setting. This option is the same as executing the `clear config` command from Privileged EXEC mode. You are not prompted to confirm the selection.

Erase Permanent Storage

Use option 3 to completely erase the switch software application, any log files, and any configurations. The boot loader and operating system are not erased. Use this option only if a file has become corrupt and you are unable to use option 2, Load Code Update Package, to load a new image onto the switch. After you erase permanent storage, you must download an image to the switch; otherwise, the switch will not be functional.

Activate Backup Image

Use option 4 to activate the backup image. The active image becomes the backup when you select this option. When you exit the Startup Utility and resume the boot process, the switch loads the image that you activated, but NetApp recommends that you reload the switch so it can perform an entire boot cycle with the newly active image.

After you activate the backup image, the following information appears:

```
Image image1 is now active.  
Code update instructions found!  
  
Extracting kernel and rootfs from image1  
Copying kernel/rootfs uimage to boot flash area  
Activation complete  
  
image1 activated -- system reboot recommended!  
Reboot? (Y/N) :
```

Enter y to reload the switch.

Start Diagnostic Application

Option 5 is for field support personnel only. Access to the diagnostic application is password protected.

Reboot

Use option 6 to restart the boot process.

Glossary

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ARP	Address Resolution Protocol
CIST	Common and Internal Spanning Tree
CLI	Command-Line Interface
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
GARP	Generic Attribution Registration Protocol
giaddr	This field indicates the relaying gateway in a DHCP packet
GVRP	GARP VLAN Registration Protocol

IGMP	Internet Group Management Protocol
IVL	Independent VLAN
LACP	Link Aggregation Control Protocol
MAC	Media Access Control
Mirror Port	Source Mirror Port (that is, the port that mirrors to probe)
Mirroring Port	Destination Mirror Port
MDIX	Management Dependent Interface Crossover
Monitor Port	Destination Mirror Port (that is, the port with probe attached)
MSTP	Multiple Spanning Tree Protocol
NIM	Network Interface Manager
PAE	Port Access Entity
Probe port	Destination Mirror Port (that is, the port with probe attached)
QoS	Quality of Service

RADIUS	Remote Authentication Dial In User Service
RSTP	Rapid Spanning Tree Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access Control System
TDR	Time Domain Reflectometry
VLAN	Virtual LAN

Index

Numerics

10/100/1000BASE-T ports, connecting to 26
802.1AX 13
802.1X 14

A

AC outlet 26
ACLs 14
acronyms 3
auto-MDIX 7, 26
auto-negotiation 7

B

backup image, activating 38
baud rate 31
 default 7
boot process 35
BOOTP client, enabling 32

C

CLI 30
CLI access
 console port 31
command mode
 Privileged EXEC 31, 37
 User EXEC 37
command prompt 31
components, hardware 6
configuration
 erase 38
 saving changes to 33
console port 7
 accessing the CLI 31
 connecting to 27
 location 6
contents, package 20
conventions, document 3

D

depth, chassis 16
DHCP client, enabling 32
diagnostic application, starting 39
dimentions, switch 16
document conventions 3
dot1x 14
dual image 10
duplex mode 7

E

environmental specification 16
erase current configuration 38
erase permanent storage 38

F

fans 8
FASTPATH application, starting 38

G

gigabit Ethernet ports 7

H

hardware
 components 6
 installation 19
height, chassis 16
humidity, acceptable 16

I

IEEE 802.1X 14
IEEE 802.3 protocols and standards, supported 16
IGMP snooping 13
image
 active and backup 10
 backup, activating 38
installation, switch 22
IP address, static 33

IPv6 management 11
ISDP 13

L

layer 2 features 12
LED
 locations 6
 RJ-45 port 8
 system 9
link aggregation 13
LLDP 13
local management 30
login 37

M

management ACL 15
management interface
 accessing 30
management, IPv6 11
management, local and remote 30
modes, command 37
MSTP 13

N

network information, configuring 30

O

outlet, power 26

P

package contents 20
password, default 31
permanent storage, erasing 38
port
 console 7, 27
 gigabit Ethernet 7
 LED definitions 8
 mirroring 13
 RJ-45 26
port channels 13
POST 35

power
 connecting 26
 controlling 26
power specification 17
power supply 8
Power-On Self-Test 35
Privileged EXEC mode 31, 37
prompt, command 31
protocols, IEEE 802.3 16

Q

QoS features 14

R

rack-mounting 22
RADIUS client 14
reboot
 from the CLI 35
 from the Startup Utility 39
remote management 30
RJ-45 port LED 8
RS-232 7

S

security features 14
site preparation 20
SNMP 10, 30
software features 10
spanning tree, multiple 13
specification, environmental 16
SSH 10, 30
standards, IEEE 802.3 16
Startup Utility
 functions 38
 menu, accessing 35
static IP address 33
switching features 12
system features 10
system LED definitions 9

T

TACACS+ client 15

- technical specifications 16
- telnet 10, 30
- temperature
 - operating 16
 - storage 16
- terminal, VT100/ANSI 27
- terminal-emulation settings 31
- terms, definitions 3
- TFTP 10
- tools and equipment, installation 21

U

- User EXEC mode 37
- user name, default 31

V

- VLAN 12

W

- weight, chassis 16
- width, chassis 16

