



IBM System Storage N series **10G Cluster-Mode Switch Installation Guide**

GI13-2866-00
NA 210-06282_B0

Copyright and trademark information

Copyright information

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

Portions copyright © 2013 IBM Corporation. All rights reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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 <http://www.ibm.com/legal/copytrade.shtml>

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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, SnapMigrator, 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.

Broadcom®, the pulse logo, Connecting everything®, the Connecting everything logo, and FASTPATH® are among the trademarks of Broadcom Corporation and/or its affiliates in the United States, certain other countries and/or the EU.

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.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at: <http://www.ibm.com/ibm/licensing/contact/>

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on

generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Table of Contents

Chapter 1	CN1610 Switch Features	5
	Hardware components	6
	Software features	12
	Technical specifications	18
Chapter 2	Hardware Installation.	21
	Before you begin	22
	Installing the switch	24
	Connecting to ports and power	28
	Installing and removing hardware components	30
Chapter 3	Switch Management.	33
	Accessing the management interface.	34
	Boot process	42
	Startup Utility functions	45
	Glossary	47
	Index	51

About this guide

Purpose and audience

This guide provides an overview of the CN1610 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 47.

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 CN1610:

- ◆ The *CN1610 Network Switch CLI Command Reference* describes the commands available from the command-line interface (CLI) for managing, monitoring, and configuring the switch.
- ◆ The *CN1610 Network Switch Administrator’s Guide* contains step-by-step configuration examples for several features.

About this chapter This chapter describes the CN1610 switch hardware components and software features and provides technical specifications.

Topics in this chapter This chapter includes the following topics:

- ◆ “[Hardware components](#)” on page 6
- ◆ “[Software features](#)” on page 12
- ◆ “[Technical specifications](#)” on page 18

CN1610 summary The CN1610 is a high bandwidth, managed Layer 2 switch that provides 16 10-Gigabit Small Form-Factor Pluggable Plus (SFP+) ports. The switch includes redundant power supplies and fan trays that support hot swapping for high availability.

This 1U switch can be installed in a standard 19-inch IBM N series 42U system cabinet or third-party cabinet.

The switch supports local management through the console port or remote management by using Telnet or SSH through a network connection. The CN1610 includes a dedicated 1-Gigabit Ethernet RJ45 management port for out-of-band switch management. You can manage the switch by entering commands into the command-line interface (CLI) or by using an SNMP-based network management system (NMS).

Hardware components

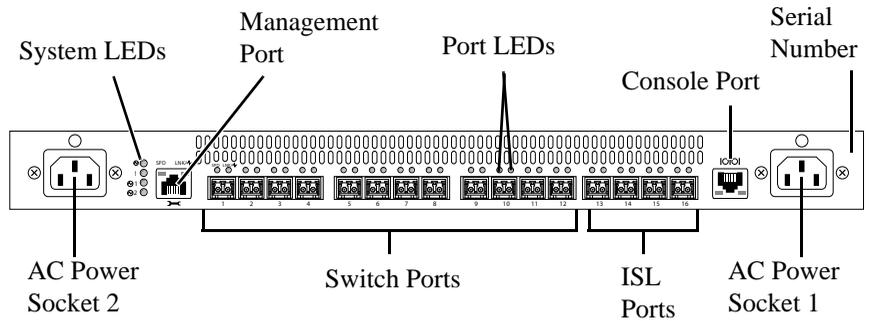
Physical description

The CN1610 has a 1U chassis design and is rack-mountable in a standard 19-inch equipment rack or an IBM N series 42U System Cabinet.

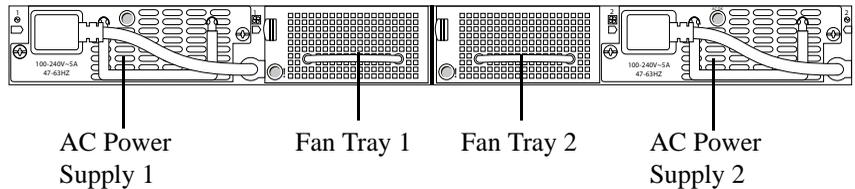
The rear panel of the switch provides the following components:

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

The following figure shows the rear panel of the switch:



The front panel provides access to the power supplies and fan trays:



SFP+ ports

The CN1610 has 16 built-in 10-Gbps SFP+ ports that provide up to 256 Gbps switching bandwidth (512 Gbps duplex).

Each SFP+ port is capable of supporting the following transceiver modules:

- ◆ 10GBase-Cu (direct attach SFP+ twinax copper cable)
- ◆ 10GBase-SR (short range optical fiber)

Four 10G SPF+ direct attach cables are included in the shipping package. Other transceivers and cables are sold separately.

Remote management port

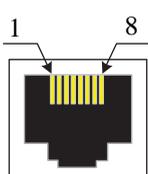
The remote management port is a 10/100/1000Base-T Ethernet port dedicated to remote switch management. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.

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).

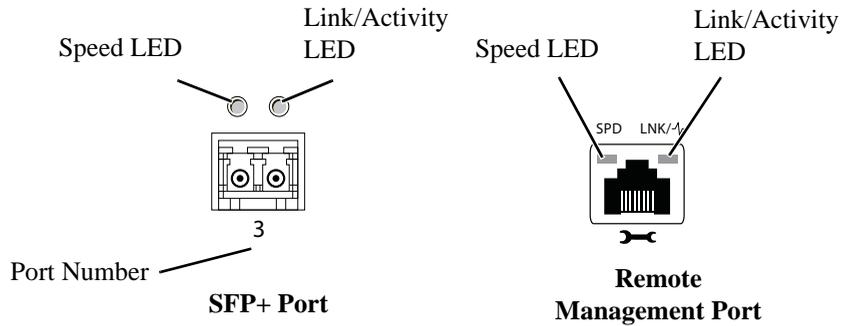
The console port supports asynchronous data of eight data bits, one stop bit, no parity bit, and no flow control. The default baud rate is 9600 bps.

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 SFP+ port has two built-in LEDs that provide port link, activity, and speed information. Similarly, the remote management port has two built-in LEDs that provide information about the port link, activity, and speed.

For the switch ports and remote management port, the Speed LED is on the upper left side of the port, and the Link/Activity LED is on the upper right side of the port:



The following table describes the Speed and Link/Activity LEDs found above each SFP+ port:

SFP+ port LED	Color	Description
Speed	Solid green	A valid 10 Gbps link is established on the port.
	Off	No link or a valid 1 Gbps link is established on the port.
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.

The following table describes the Speed and Link/Activity LEDs found above the remote management port:

Management port LED	Color	Description
Speed	Solid green	A valid 1000 Mbps link is established on the port.
	Solid amber	A valid 100 Mbps link is established on the port.
	Off	No link or a valid 10 Mbps link is established on the port.
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.

Power supplies

The CN1610 has two internal, replaceable AC power supplies for redundant or load-sharing operation. Each power supply can provide 300 watts and includes hot-swap support.

Each power supply receives power by connecting an AC power source to the power socket on the rear panel of the switch.

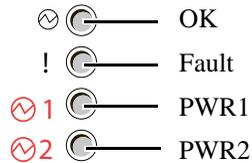
Although the cluster network switch has redundant power supplies and can operate normally when only one power supply is installed and operational, IBM recommends that you replace any failed power supply immediately to maintain redundancy. If one power supply fails, a second power supply must be present and functional for the switch to continue to operate.

Fan units

The two fan trays in the CN1610 support hot-swapping and can be removed or inserted from the front panel. Each fan tray includes two fans. For the switch to maintain an acceptable operating temperature, both fan trays must be present in the chassis, and all four fans must be operational.

System LED definitions

The system LEDs provide information about the overall system status, fan status, and power-supply status. The following figure identifies each system LED:



The following table describes the system LEDs:

System LEDs	Color	Description
 OK	Solid green	The switch DC power (all low-voltage supplies from 3.3 to 1.0V except the standby DC voltage) is operating normally.
	Blinking green	The switch is booting, and power-on self test (POST) is in progress.
	Blinking amber	The switch has experienced one or more DC power faults.
	Off	A standby DC fault is detected.
 Fault	Solid amber	One or more fan failures have occurred.
	Off	The fans are operating normally.
 PWR1	Solid amber	Power supply 1 has a fault or is missing.
	Off	Power supply 1 is present and operating normally.
 PWR2	Solid amber	Power supply 2 has a fault or is missing.
	Off	Power supply 2 is present and operating normally.

In addition to the system LEDs on the back panel of the switch, each fan tray and power supply includes LEDs on the front panel to provide status information:

Front-panel LEDs	Color	Description
 AC OK	Solid green	The AC power supply has power.
	Off	The AC power supply does not have power.
 Fan	Amber	A fan fault has been detected.
	Off	The fan is operating normally.

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	The switch supports the following IPv6 management protocols and applications: <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)	The switch supports the following four groups defined as part of the RMON standard: <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
IEEE 802.3x flow control	Allow lower speed switches to communicate with higher speed switches by handling requests for the higher speed switch to refrain from sending packets. Transmissions are temporarily halted to prevent buffer overflows.
Port control	Configure individual port settings such as administrative status, speed, duplex, and autonegotiation mode.
Jumbo frames	On a per-port basis, extend the maximum frame size (Ethernet MTU) that a port can transmit from 1518 bytes (1522 bytes with VLAN header) to up to 9216 bytes.
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.

Switching feature	Description
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.
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.

Switching feature	Description
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
Class of Service (CoS) queuing	Directly configure certain aspects of the hardware traffic queueing to affect QoS behavior for different types of network traffic. CoS queue characteristics such as minimum guaranteed bandwidth and transmission rate shaping are configurable at the queue (or port) level.
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.
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 CN1610 switch:

Specification	Measurement
Height	43 mm (1.69 in)
Width	445 mm (17.5 in)
Depth	508 mm (20 in)
Weight	10.2 kg (22.5 lbs)

Network protocol and standards compatibility

The CN1610 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
- ◆ IEEE 802.3z 1000Base-X
- ◆ IEEE 802.3ae 10 Gpbs Ethernet over fiber

Environmental specification

The following table lists the environmental specification for the CN1610 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 CN1610 switch:

Specification	Measurement
AC-input frequency (universal)	50 to 60 Hz
AC-input voltage (universal)	100 to 240 VAC
Power supply	300W
DC-output voltage	12V

About this chapter This chapter contains information about preparing to install the CN1610 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 22
- ◆ [“Installing the switch”](#) on page 24
- ◆ [“Connecting to ports and power”](#) on page 29
- ◆ [“Installing and removing hardware components”](#) on page 31

Before you begin

Site preparation

The location and conditions of the place where you decide to install the CN1610 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 18.
- ◆ 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 port to the connected device must not exceed 328 feet (100 meters).
- ◆ The cable length from the SFP ports must not exceed recommended lengths for the cable and transceiver module type.
- ◆ 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 CN1610 package includes the following contents:

- ◆ CN1610 switch
- ◆ Software license and warranty information
- ◆ Rack-mount installation kit
- ◆ RJ45 to DB-9 console cable
- ◆ Four SFP+ direct attach copper cables

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

The following table lists the parts included in the slide rail box:

Description	Quantity
Support rails	2(left and right)
M5 screws	10
M5 nut-clips	10
10-32 screws	2*

*These screws may not be included in the slide rail box. If you do not find the 10-32 screws in the slide rail box, please check for them in the CN1610 package kit.

Required tools and equipment

Before installing the switch in a standard equipment rack or IBM N series 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

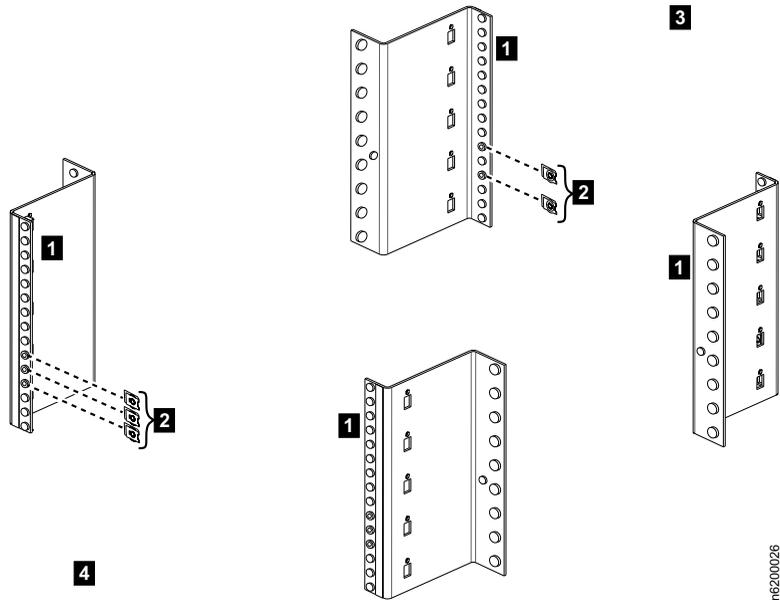
Rack-mounting the switch

The switch can be installed on a 2101-N42 rack. The rack has the following features:

- ◆ Four posts
- ◆ Flanges provided with round holes

To install the switch on a 2101-N42 four-post rack:

1. Fix three clip nuts to the front rack and two-one to the top and the other to the bottom hole-of the rear rack. Fix the clip nuts to both the left and the right racks. The diagram below shows the four-post rack and the clip nuts that are to be clamped sideways onto the flanges of the rack.

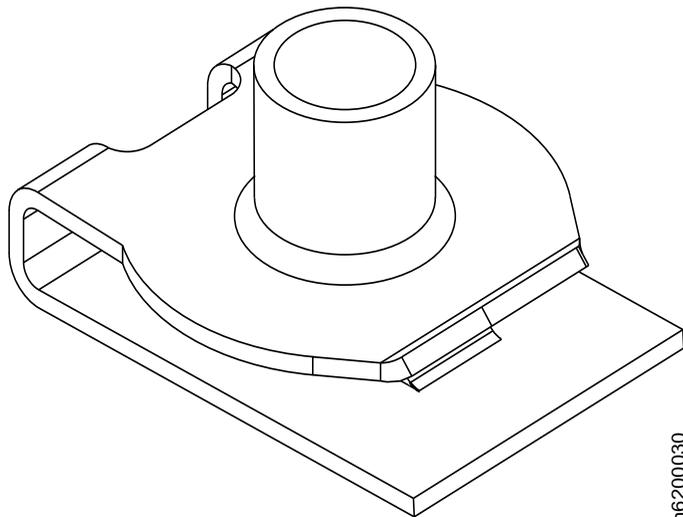


The table below lists the label descriptions for the diagram.

Label	Description
1	The flanges of the rack

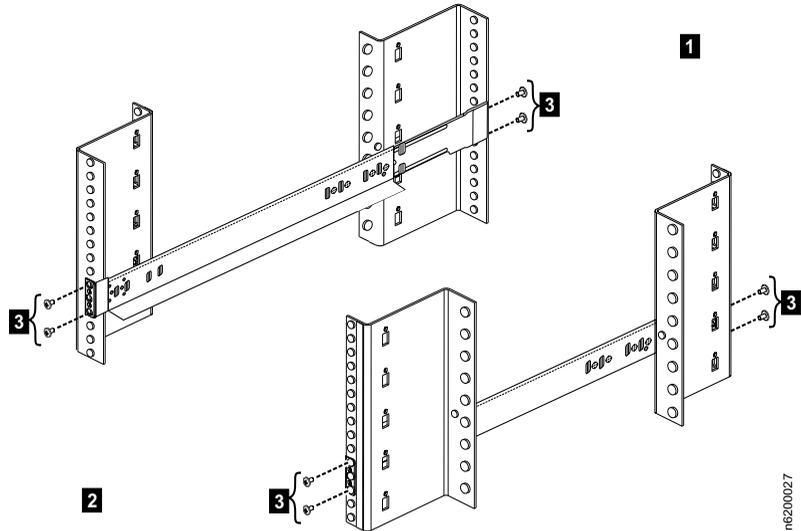
Label	Description
2	The nut clips to be clamped sideways onto the flanges of the rack
3	The rear portion of the rack
4	The front portion of the rack

The diagram below illustrates the part of the nut clip that must be on the inner side of the flange after the nut clip is clamped sideways onto the flange.



n6200030

- Fix the left and right rails onto the rack. Use two M5 screws to fix the front and two M5 screws to fix the rear of each rail onto the rack.

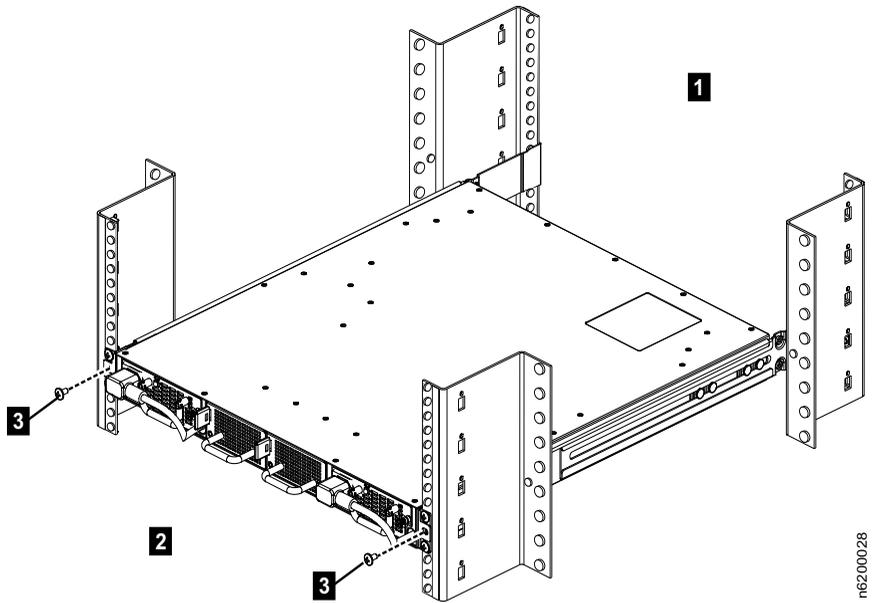


m6200027

The table below lists the descriptions for each label in the diagram.

Label	Description
1	The rear portion of the rack
2	The front portion of the rack
3	The M5 screws used to fix the rails onto the rack

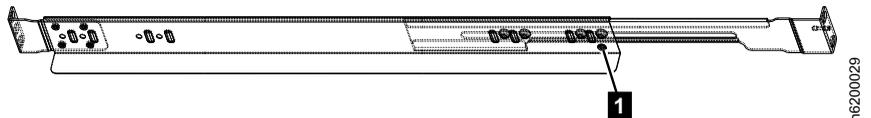
- Slide the switch onto the supporting rails until the support brackets (on both sides of the switch) touch the front flanges. Fix the front side of the switch to the rails by using two M5 screws.



The table below lists the descriptions for each label in the diagram.

Label	Description
1	The rear portion of the rack
2	The front portion of the rack
3	The M5 screws used to fix the front side of the switch to the rails.

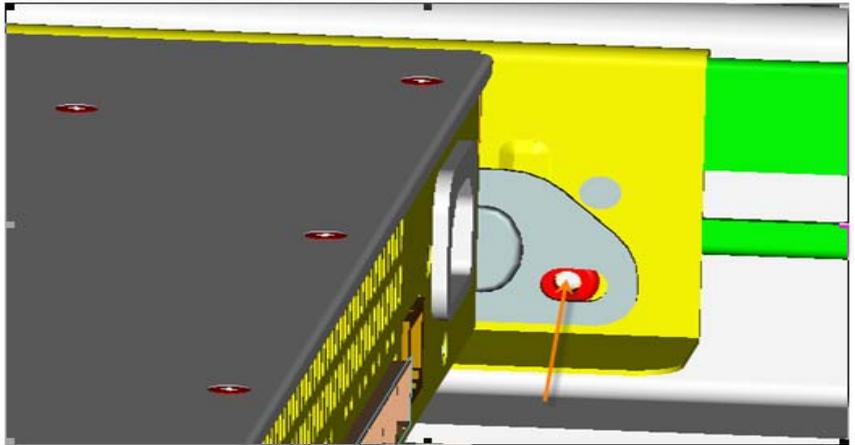
Ensure that the switch is well-seated. Use two 10-32 screws (one for each side) to fix the rear end of the switch to the tie-down feature on the rail. The diagram below is of a left rail.



The table below lists the description for the label in the diagram.

Label	Description
1	The location of the tie-down feature on the left rail

The illustration below displays the alignment of the rear bracket with the tie-down hole. The arrow indicates where the 10-32 screw must be fitted in.



Connecting to ports and power

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

Use Category 5 (Cat5) Unshielded Twisted-Pair (UTP) cable terminated with an RJ-45 connector to connect to the 10/100/1000BASE-T Ethernet port for remote network management. 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 to the SFP+ ports

SFP+ copper twin-ax cables connect directly into the SFP+ port and do not require a separate SFP+ transceiver module. If you use an optical cable for 10GBase-SR transmissions, install the appropriate transceiver module before connecting the fiber-optic cable between the switch and the target device, see [“Installing and removing SFP+ modules”](#) on page 31.

After the SFP+ transceiver module has been installed in the SFP+ port, connect one end of the appropriate fiber-optic cable to the module installed in the switch port, and connect the other end to the target device.

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

Connecting power to the switch

The CN1610 switch does not have an ON/OFF switch. Power to the switch is controlled by the power cord connection. The switch can be powered by a single power source, but it is recommended that you connect each power supply to separate AC circuits for load sharing and redundancy. You can connect power to the power sockets on the front or back panel of the switch.

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. For each power supply, connect the end of the power cable to the power receptacle on the rear panel of the switch.

Note

The built-in power cables on the power supply front panels should always be connected.

2. Connect the power cord to the power source.
3. Verify that the AC OK LED on each power supply 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 35.

Installing and removing hardware components

Installing and removing SFP+ modules

Note

SFP+ transceiver modules are sold separately.

The following procedures describe how to install a SFP+ transceiver module into one of the SFP+ ports of the switch.

CAUTION

Disconnect all cables from the SFP+ transceiver before installing or removing it from the SFP+ port.

CAUTION

To prevent ESD damage to the module, wear a properly-grounded antistatic wrist strap while handling the module.

1. Holding the SFP+ module by its sides, identify the top side of the SFP+ module.
2. Align the module with the port.
3. Insert the module securely into the SFP port until it clicks into place in the rear of the slot.

Use minimal pressure when inserting the transceiver to avoid damage.

To remove the SFP+ module, disconnect the cable from the module and gently but firmly pull it out of the port.

Removing and installing a power supply

The switch is intended to operate with both power supplies connected to separate AC power circuits to provide power load sharing and redundancy. However, if a power supply fails the switch continues to operate normally.

CAUTION

If a power supply fails, replace it immediately to maintain power redundancy.

You can remove and replace a power supply without removing power from the switch.

To remove and replace a power supply, follow these steps:

1. Disconnect the power cord from the appropriate power socket on the rear panel of the switch.
2. On the switch front panel, use your fingers to turn the two thumb screws counter-clockwise and loosen the screws.
3. Using the handle, pull the power supply out of the chassis.
4. Insert the new power supply in the chassis until it is firmly seated.
5. Tighten the screws by turning them clockwise.
6. On the switch rear panel, connect the power cord between the AC power source and the power socket on the power supply.
7. Verify that the AC OK LED on the power supply is green, which indicates that the power supply is providing power to the switch.

Removing and installing a fan tray

For the switch to maintain an acceptable operating temperature, the four fans (two in each fan tray) must be operational. If any fan fails, the fault LED on the rear panel of the switch is amber, and the fan tray with the failed fan must be replaced.

CAUTION

If any fan unit fails, replace the fan tray immediately to ensure that the switch operates at an acceptable temperature.

You can remove and replace a fan tray without removing power from the switch.

To remove and replace a fan tray, follow these steps:

1. Push and hold the fan tray release lever to the right.
2. The release lever is located on the left side of the fan tray.
3. Using the handle, pull the fan tray out of the chassis.
4. Insert the new fan tray in the chassis until it is firmly seated and the green LED on the fan tray illuminates.

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 *CN1610 Network Switch CLI Command Reference* and the *CN1610 Network Switch Administrator's Guide*.

Topics in this chapter

This chapter includes the following topics:

- ◆ “[Accessing the management interface](#)” on page 34
- ◆ “[Boot process](#)” on page 42
- ◆ “[Startup Utility functions](#)” on page 45

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.

In-band and out-of-band management

The CN1610 has a port intended solely for out-of-band switch management. This 10/100/1000Base-T port is known as the remote management port or service port. Traffic received on the remote management port is never switched to any in-band (network) port. Likewise, traffic received on any in-band port is never forwarded or routed over the remote management port.

Alternatively, you may choose to manage the switch through the production network. This in-band management is possible through any SFP+ port that has a network connection. Because in-band management traffic is mixed in with production network traffic, it is subject to all of the filtering rules usually applied on a switched/routed port such as ACLs and VLAN tagging.

The features available on the management port are limited to protocols required to manage the switch, for example Telnet, SSH, DHCP client, and TFTP. Limiting the configuration options makes it difficult to accidentally cut off management access to the switch.

If the production network is experiencing problems, you can still use the remote management port to access the switch management interface and troubleshoot issues.

Note

It is recommended that you connect the remote management port to the management network for out-of-band management.

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. DHCP is enabled by default on the management port. The DHCP client on the network ports is disabled by default. For more information on configuring the network see the *Clustered Data ONTAP Switch 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
- ◆ View network information that has been dynamically assigned to the management port by the DHCP server on your network. If you manage the switch by using a network port, you must manually disable the DHCP client on the management port and enable the DHCP client on the network ports.

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 42.

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 *Clustered Data ONTAP Switch Setup and Configuration Guide*.

After a successful login, the screen shows the system prompt, for example (CN1610) >.

5. At the (CN1610) > 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 (CN1610) #.

For information about the command modes, see the *CN1610 Network Switch CLI Command Reference*.

Note

DHCP is enabled by default on the remote management port.

Viewing and configuring remote management port information

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. The procedures in this section describe how to view network information configured on the remote management port and, optionally, enable the DHCP, BootP, or DHCPv6 client if necessary. For information about similar procedures to allow the switch to be managed over the production network, see [“Enabling the DHCP or BootP client for in-band management”](#) on page 39.

To view the management port network information and (optionally) configure the remote management port 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 35.
2. Use the `show serviceport` command to view the network information assigned to the switch by the network server:

```
(CN1610) #show serviceport
Interface Status..... Up
IP Address..... 10.27.22.196
Subnet Mask..... 255.255.252.0
Default Gateway..... 10.27.20.1
IPv6 Administrative Mode..... Enabled
```

```
IPv6 Prefix is ..... fe80::210:18ff:fe82:1994/64
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
Burned In MAC Address..... 00:10:18:82:19:94
```

3. If the default configuration has been changed and the DHCP or BootP client has been disabled, use the following procedures to enable the DHCP, BOOTP, or DHCPv6 client on the switch:

- ❖ To enable DHCP, enter the following command from Privileged EXEC mode:

```
serviceport 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:

```
serviceport protocol bootp
```

- ❖ To enable the DHCPv6 client on the switch, enter the following command:

```
serviceport ipv6 address dhcp
```

4. Optionally, save the current configuration so that all changes are retained during a switch reset:

```
write memory
```

Configuring static network information on the remote management port

Use the following procedures to manually configure a static IPv4 address, subnet mask, and default gateway on the remote management port. For information about configuring static information so that the switch can be managed over the production network, see [“Configuring static network information for in-band management”](#) on page 40.

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 35.

2. To disable the DHCP client on the port, enter:

```
serviceport protocol none
```

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

```
serviceport ip 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:

```
serviceport ip 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:

```
serviceport ipv6 address ipv6-address/prefix-length [eui64]
```

```
serviceport 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:

```
serviceport ipv6 address 2001:DB8:132::3/32
```

```
serviceport ipv6 gateway 2001:DB8:132::1
```

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

```
(CN1610) #show serviceport
```

```
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
DHCPv6 Client DUID ..... 00:03:00:06:00:10:18:82:06:4C
Configured IPv4 Protocol ..... None
Configured IPv6 Protocol ..... None
IPv6 Autoconfig Mode..... Disabled
Burned In MAC Address..... 00:10:18:82:06:4C
```

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

```
write memory
```

Enabling the DHCP or BootP client for in-band management

Although it is recommended that you manage the switch by using the remote management port, you can manage the switch over the production network through any of the SFP+ switch ports. The procedures in this section describe how to configure the in-band management interface. For information about similar procedures to allow out-of-band management, see [“Viewing and configuring remote management port information”](#) on page 36.

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 35.

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:

```
(CN1610) #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 for in-band management

Use the following procedures to manually configure a static IPv4 address, subnet mask, and default gateway on the in-band management interface. For information about similar procedures to enable out-of-band management, see [“Configuring static network information on the remote management port”](#) on page 37.

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 35.
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:

```
(CN1610) #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 45.

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 35.
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 - Select Boot Method
5 - Activate Backup Image
6 - Start Diagnostic Application
7 - Reboot

Q - Quit from FASTPATH Startup
```

For information about the options available from the menu, see “[Startup Utility functions](#)” on page 45.

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 *CN1610 Network Switch CLI Command Reference* and the *CN1610 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.

Select Boot Method

Use option 4 to specify whether the system should boot from the image stored on the internal flash, from an image over the network, or from an image over the serial port. By default, the switch boots from the flash image.

To boot over the network, the image must be located on a TFTP server that can be accessed by the switch. To boot from the serial port, the switch must be connected through the console port to a terminal or system with a terminal emulator. The image must be located on the connected device.

If you select option 4, the following menu appears:

```
Current boot method: FLASH
```

- 1 - Flash Boot
- 2 - Network Boot
- 3 - Exit without change

```
Select option (1-3):
```

If you select a new boot method, the switch uses the selected method for the next boot cycle.

Activate Backup Image

Use option 5 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 IBM 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 6 is for field support personnel only. Access to the diagnostic application is password protected.

Reboot

Use option 7 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 28
802.1AX 15
802.1X 17

A

AC outlet 29
ACLs 16
acronyms 3
auto-MDIX 28

B

backup image, activating 46
baud rate 35
 default 7
boot method, selecting 45
boot process 42
BOOTP client, enabling 39
 remote management port 36

C

CLI 34
CLI access
 console port 35
command mode
 Privileged EXEC 36, 43
 User EXEC 43
command prompt 36
components, hardware 6
configuration
 erase 45
 saving changes to 40
console port 7
 accessing the CLI 35
 connecting to 29
 location 6
contents, package 22
conventions, document 3
CoS 16

D

depth, chassis 18
DHCP client, enabling 39
 remote management port 36
diagnostic application, starting 46
dimensions, switch 18
direct attach cables 7
document conventions 3
dot1x 17
dual image 12

E

environmental specification 18
erase current configuration 45
erase permanent storage 45

F

fan tray, removing and installing 31
fans 9
FASTPATH application, starting 45
flow control 14
frames, jumbo 14

H

hardware
 components 6
 installation 21
height, chassis 18
hot-swap
 fan 9
 power supply 9
humidity, acceptable 18

I

IEEE 802.1X 17
IEEE 802.3 protocols and standards, supported 18
IEEE 802.3x 14
IGMP snooping 15

- image
 - active and backup 12
 - backup, activating 46
- in-band management 34
- installation, switch 24
- IP address, static 37, 40
- IPv6 management 13
- ISDP 15

J

- jumbo frames 14

L

- layer 2 features 14
- LED
 - locations 6
 - remote management port 9
 - SFP+ Port 8
 - system 10
- link aggregation 15
- LLDP 15
- load sharing, power 30
- local management 34
- login 43

M

- management ACL 17
- management interface
 - accessing 34
 - in-band and out-of-band 34
- management port
 - LED 9
 - location 6
- management, IPv6 13
- management, local and remote 34
- modes, command 43
- MSTP 15
- MTU 14

N

- network information, configuring 35

O

- outlet, power 29
- out-of-band management 34

P

- package contents 22
- password, default 35
- permanent storage, erasing 45
- port
 - console 7, 29
 - LED definitions 8
 - mirroring 15
 - remote management 7
 - RJ-45 28
 - service 34
 - SFP+ 7, 28
- port channels 15
- POST 42
- power
 - connecting 29
 - controlling 29
- power specification 19
- power supply 9
 - removing and installing a 30
- Power-On Self-Test 42
- Privileged EXEC mode 36, 43
- prompt, command 36
- protocols, IEEE 802.3 18

Q

- QoS features 16

R

- rack-mounting 24
- RADIUS client 17
- reboot
 - from the CLI 42
 - from the Startup Utility 46
- redundancy, power 30
- remote management 34
- remote management port 7
 - enabling DHCP or BOOTP 36

- location 6
- static IP address 37
- RS-232 7

S

- security features 17
- service port 34
- SFP+ modules
 - installing 30
 - removing 30
- SFP+ port 7
 - connecting to 28
 - LED 8
 - supported modules 7
- SFP+ transceiver modules, supported 7
- site preparation 22
- SNMP 12, 34
- software features 12
- spanning tree, multiple 15
- specification, environmental 18
- SSH 12, 34
- standards, IEEE 802.3 18
- Startup Utility
 - functions 45
 - menu, accessing 42
- static IP address 37, 40
- switching features 14
- system features 12
- system LED definitions 10

T

- TACACS+ client 17
- technical specifications 18
- telnet 12, 34
- temperature
 - operating 18
 - storage 18
- terminal, VT100/ANSI 29
- terminal-emulation settings 35
- terms, definitions 3
- TFTP 12
- tools and equipment, installation 23
- transceiver modules, SFP+ 7
- twinax copper cable 7

U

- User EXEC mode 43
- user name, default 35

V

- VLAN 14

W

- weight, chassis 18
- width, chassis 18



NA 210-06282_B0, Printed in USA

GI13-2866-00

