Part No. 216078-A
December 2003

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the BayStack 420/425 10/100/1000 Switches, Software Version 3.0

216078-A

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

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

Trademarks

Nortel Networks, the Nortel Networks logo, the Unified Networks, BayStack 420, BayStack 425, and Optivity are trademarks of Nortel Networks.

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Java is a trademark of Sun Microsystems, Inc.

Macintosh is a trademark of Apple Computer, Inc.

Netscape Navigator is a trademark of Netscape Communications Corporation.

Restricted rights legend

Use, duplication, or disclosure by the United States 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 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Contents

Introduction

These release notes contain important information about Nortel Networks BayStack 420 10/100/1000 switch and BayStack 425 10/100/1000 switch, software version 3.0, and operational issues that is not available in the following related documents:

- *Installing the BayStack 425 10/100/1000 Switch* (part number 215658-A)

  Describes how to install the BayStack 420/425 Switch.

- *Getting Started with BayStack 425 Software* (part number 215663-A)

  Describes how to install the Device Manager software management application.

- *Reference for the BayStack 425 Management Software* (part number 215662-A)

  Describes how to use the Device Manager software management application.

- *Using the BayStack 425 10/100/1000 Switch* (part number 215661-A)

  Describes how to use the BayStack 425 10/100/1000 Switch for network configuration.

- *Using Web-based Management for the BayStack 425 10/100/1000 Switch, Software Version 3.0* (part number 215660-A)

  Describes how to use the Web-based management tool to configure switch features.

- *Reference for the BayStack 425 10/100/1000 Command Line Interface, Software Version 2.0* (part number 215659-A)

  Describes how to use Command Line Interface (CLI) commands to configure and manage the BayStack 420/425 Switch.

BayStack 420/425 10/100/1000 Switch, Software Version 3.0

This release of BayStack 420/425 10/100/1000 Switch, software version 3.0 is to support the BayStack 420 10/100/1000 and BayStack 425 10/100/1000 switch hardware.

This release includes:

- Version 3.0 of the BayStack 420/425 software
- Version 3.0 of the BayStack 420/425 diagnostics
- Version 5.7.4.0 of Device Manager

Known issues in BayStack 420/425, software version 3.0

- In the CLI, you can only configure VLAN settings on D-MLT ports by using the first port. (Q00748099)
- Traffic may not recover on DMLT ports after the base unit is reset. (Q00756907)
- You cannot disable Autonegotiation on port 25 using the CLI. (Q00758551)
- On DMLT and MLT ports, DA filtering on Intrusion Detected does not work properly. (Q00756497)
- If Bootp is in use, the “In Use” IP Address may be displayed when you enter the show running-config command. (Q00756774)
- When you configure static route ports using telnet or the console interface (Switch Configuration -> IGMP Configuration -> IGMP Configuration), you need to select the ports slowly. If you do not hold the selection for a few seconds, the ports may automatically de-select. (Q00610029)
- In Device Manager, if you refresh the dialogue box: Edit -> Security -> Auth Config: Insert MAC Address, if the Brd Indx user field is populated, it may clear (change from 1 to 0). (Q00603216)
- In an 8 high stack of BayStack 425 units, the running-config fails if you are using a TFTP server from OSM 3.0 (Win). (Q00745212)
- Max 122 IGMP groups learned on non-BU are displayed in a multicast table (Q00564442)

- If a port was disabled because mac security partition on intrusion was detected, and the device is reset, the port will remain disabled. Q00773091)
- In Device Manager, the RMON -> Alarm Manager -> Help does not display the correct page. (Q00751674)
- The link Support-> Upgrade from Web interface doesn't work. (Q00787231)
- In the CLI, From Privileged EXEC# configure network works only when it’s used in a single command. (Q00787185)
- There is no way to see snmp-server status (enable or disable). (Q00788009)
- There may be a Critical error message logged in Sys Log after retrieval of a large configuration file into the stack. However, this has no effect on the functionality of the switch. (Q00742627)
- SSH secure becomes SSH true on BS425 if the snmp-server command is enabled on a non-base unit. (Q00774868)
- When Ports get disabled with mac-security enabled feature due to detection of intruder. If the switch is shutdown with that condition, such ports would come up with disabled status. (Q00773091)
- The MIB object entPhysicalDescr does not return the correct information about inserted GBICs. (Q00808149)
- Unsupported GBICs may be displayed when you use the CLI show hardware command. (Q00774180)
- The Autotopology status cannot be displayed using the console interface, but it can be displayed using the CLI show sys-info command. (Q00707067)
- The Spanning Tree parameters on a port cannot be changed using the console interface, but they can be changed using CLI. (Q00592138-02)
- Under high traffic conditions, port error statistics may increment at a slowerrate than the actual count. (Q00436730, Q00169766)
- There may be some discrepancy between the actual amount of time it takes for MAC addresses to be aged and the configured aging time. It may be equal to or greater than the aging time that is set. (Q00436722)
- When using MAC address security, the unit will enter intruder MAC addresses in the address learning table, but those addresses will never age out. (Q00584754)
- The Device Manager allows VLAN membership to be modified after the removal of all ports from management VLAN #1. (Q00695826)
- When selecting Edit > Unit in the Device Manager, the dialog box incorrectly displays CardMda instead of Unit. (Q00696950)

- The autonegotiation advertisements feature is not supported for ports 25 or 26 in this release. (Q00697804)
- Flow control is not negotiated as part of the autonegotiation exchange for
- gigabit ethernet ports. (Q00593496)
- If an unsupported GBIC is inserted in the device, the Web-management interface will incorrectly show NONE for ports 25 and 26. (Q00699390)
- Optivity Switch Manager 3.0 does not support this device. Support will be added in Optivity Switch Manger 4.0. (Q00695751)
- It is possible for the user to accidentally disable password access to the console interface by entering the following command:

  ```
  cli password rw <username>
  ```

  This command specifies the username, which is not used by the system, but does not specify a password. This creates a null password that the user cannot enter to gain access to the CLI, locking the user out of the CLI. The correct command is:

  ```
  cli password rw <username> <password>
  ```

  The command requires that the user enter a username before they enter a password even though the username is disregarded by the system. If a null

  password is accidentally set, refer to “Restoring a lost password” for information on resetting the password. (Q00611658)
- When using the CLI to change the Spanning Tree Protocol (STP) for the switch or entire stack, STP will also be changed for the multilink trunk. The workaround is to use the console interface to change the STP. (Q00558519)
- If the Boot Mode is set to BootP Always, the MAC address FF-FF-FF-FF-FF-FF is displayed in the last position of the MAC address table. (Q00614452)
- When configuring MLT links, you must ensure that both sides of the MLT have the same STP configuration. Failure to configure both sides of the MLT with the same STP capabilities can yield unpredictable results. (Q00597129)
- When STP is disabled, BPDUs are not forwarded across the switch. (Q00703438)
- Both sides of a link must be configured identically in terms of autonegotiation, speed, duplex and flow control. You cannot disable autonegotiation on a 1000BaseT connection. You must keep autonegotiation enabled on copper Gigabit ports. (Q00716500)

- When a port is administratively disabled, the port will still provide a link signal to the connected device. (Q00728619)
- The following SNMP objects refer to features that have not been implemented:

  rcVlanProtocolId

  rcVlanSubnetMask

  rcVlanPortDiscardTaggedFrames

  dot1qPortIngressFiltering

  (Q00687734)

  When attempting to change the speed while the switch is running at a high rate of traffic, the Spanning Tree Protocol (STP) does not work properly for a configuration containing two redundant links. To change the speed: disable the links, change the speed, and then re-enable the links. (Q00691614)

Restoring a lost password

> **Note:** The following procedure changes your switch to default values. All of the switch configuration information will be lost.

To restore a lost password, do the following

1. Attach a console cable to the serial port
2. Start your terminal emulation program
3. Apply power to the switch
4. As the switch begins to initialize, press CTRL-C on your keyboard. You should see a listing of information. For example:

```
BayStack 425 Switch Diagnostics 3.0.0.0

Testing main memory - PASSED

>> Break Recognized - Wait..

Resets: 142.
```

```
Initializing Flash..

Reading MAC  Address..

MAC Address: 00:E0:7B:CC:78:C0

Initializing Switch CBs,....

Initializing Switch HW..

Press 'a'  to run Agent code

Press 'd'  to Download agent code

Press 'e'  to display Errors

Press 'i'  to Initialize config/log flash

Press 'p'  to run POST tests..
```

5. Press ‘i’ to initialize the configuration. This erases the password and the configuration.

   The following prompt is displayed:

   ```
   Erase Config/Log Flash? y/N [ N ]:
   ```

6. Press Y

   The following information is displayed:

   ```
   Erasing     - Wait 0  sec..

   Press 'a'  to run Agent code

   Press 'd'  to Download agent code

   Press 'e'  to display Errors

   Press 'i'  to Initialize config/log flash

   Press 'p'  to run POST tests..
   ```

7. Press ‘a’.

Important Notes for Software Version 3.0

Stacking

With software version 3.0, the stacking capability of the BayStack 425 switch is enabled.

With software version 3.0 you can stack BayStack 420 or BayStack 425 switches, or have mixed stacks of both BayStack 420 and BayStack 425 switches.

In a mixed stack, the base unit must be a Baystack 425 switch and the BayStack 425 and BayStack 420 switches cannot be interlaced. All of the BayStack 425 switches in the stack must be stacked together and all of the BayStack 420 switches must also be stacked together.

Use the following CLI commands to set the stacking mode:

- `stacking-mode [enable|disable]` to set the stack to standalone mode (disable) or to stack - no base unit mode (enable)
- `stacking-mode base [enable|disable]` to enable base unit mode (enable) or disable base unit mode (disable)

You must reset the switch to apply the new stacking-mode configuration to both the CLI and the User Interface Button. The switch maintains the stacking-mode configuration after it is set to default.

Front Panel User Interface Button

The User Interface button on the front panel of the BayStack 425 10/100/1000 Switch is enabled in software version 3.0.

The User Interface button allows you to:

- Set the switch as the base unit in stacking mode
- Set the switch as a non-base unit in stacking mode
- Reset a stack or unit
- Put the switch in standalone mode

The UI Button's configuration is stored in flash as a part of the configuration file. The CLI command `show stacking-mode` displays information about the the stacking mode:

- Standalone
- stackable - base unit not set
- stackable - base unit set

To use the User Interface button, do the following:

1. Press the User Interface button for 3 seconds to enter Command Mode.
2. Press the button one time to select a unit as the base unit in stacking mode time, or press the button 2 times to set the unit as a non-base unit in stacking mode.
3. To reset a unit, press the User Interface button 3 times.
4. To specify no operation, press the User Interface button 4 times.
5. To place a unit in standalone mode, press the User Interface button 5 times.
6. To execute a command, press the User Interface button for 3 seconds after the selection has been made.
7. To exit command mode for the User Interface, press the button 6 times, or execute the command, or wait 20 seconds.

Small Form Factor Pluggable (SFP) GBIC and 1000BaseT ports

The BayStack 425 10/100/1000 Switch provides two SFP-GBIC ports and two 1000BaseT ports instead of one GBIC port like the BayStack 420 does.

The SFP GBIC and the 1000BaseT connectors of port 25 share resources. Only one of the two connectors for port 25 is active at any one time.

The SFP GBIC and 1000BaseT connectors of port 26, and the stack connector on the back of the unit all share resources.

Neither the SFP GBIC nor the 1000BaseT connector for port 26 is available if stacking is enabled. If stacking is disabled, only one of the two connectors for port 26 will be active.

Secure Shell (SSH)

This section covers the following topics:

- “Overview,” (next)
- “Configuring SSH using the Nortel Networks Command Line Interface (NNCLI)” on page 18

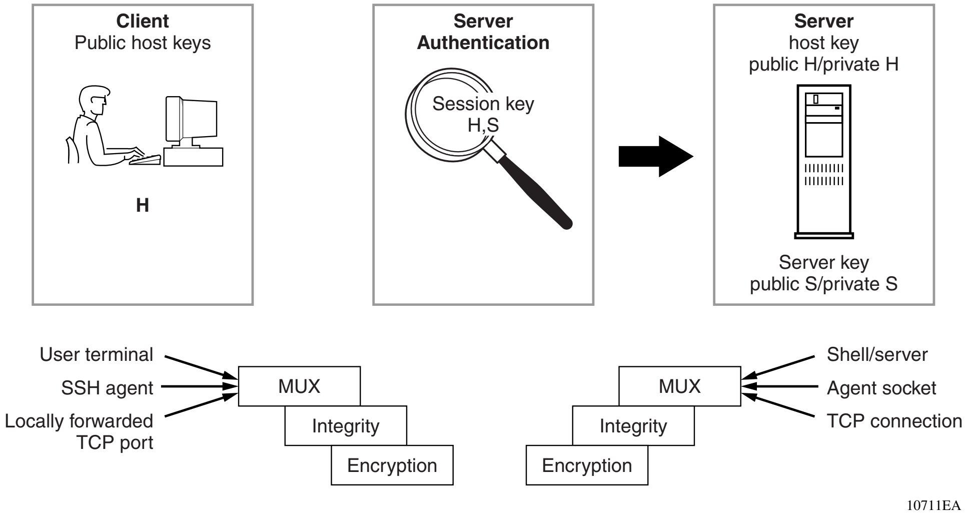
Overview

Secure Shell (SSH) is a client/server protocol that specifies the way to conduct secure communications over a network. When using other methods of remote access, such as Telnet or FTP, the traffic generated by these utilities is not encrypted. Anyone who can see the network traffic can see all data, including passwords and user names. SSH can replace telnet, ftp, and other remote logon utilities with an encrypted alternative.

In addition to standard username/password authentication, SSH supports a variety of the many different public/private key encryption schemes available. Using the public key of the host server, the client and server negotiate to generate a session key known only to the client and the server. This one-time key is then used to encrypt all traffic between the client and the server.

Figure 1 gives an overview of the SSH protocol.

Figure 1 Overview of the SSH protocol



Using a combination of host, server, and session keys, the SSH protocol can provide strong authentication and secure communication over an insecure network, offering protection from the following security risks:

- IP Spoofing
- IP source routing
- DNS spoofing
- Man-in-the-middle/TCP hijacking attacks
- Eavesdropping/Password sniffing

Even if network security is compromised, traffic cannot be played back or decrypted and the connection cannot be hijacked.

The secure channel of communication provided by SSH does not provide protection against break-in attempts or denial-of-service (DoS) attacks.

The SSH protocol supports the following security features:

- Authentication—This determines in a reliable way to identify the SSH client. During the login process the SSH client is queried for a digital proof of identity.

Supported authentications are DSA and passwords.

- Encryption—The SSH server uses encryption algorithms to scramble data and rendered it unintelligible except to the receiver.

  Supported encryption is 3DES only.

- Integrity—This guarantees that the data is transmitted from the sender to the receiver without any alteration. If any third party captures and modifies the traffic, the SSH server will detect this alteration.

The implementation of the SSH server on the BayStack 420/425 Switch enables the SSH client to make a secure connection to BayStack 420/425 Switch and will work with commercially available SSH clients.

SSH version 2 (SSH-2)

SSH protocol, version 2 (SSH-2) is a complete rewrite of the SSH-1 protocol. While SSH-1 contains multiple functions in a single protocol, in SSH-2 the functions are divided among three layers:

- SSH Transport Layer (SSH-TRANS)

  The SSH transport layer manages the server authentication and provides the initial connection between the client and the server. Once established, the transport layer provides a secure, full-duplex connection between the client and server.

- SSH Authentication Protocol (SSH-AUTH)

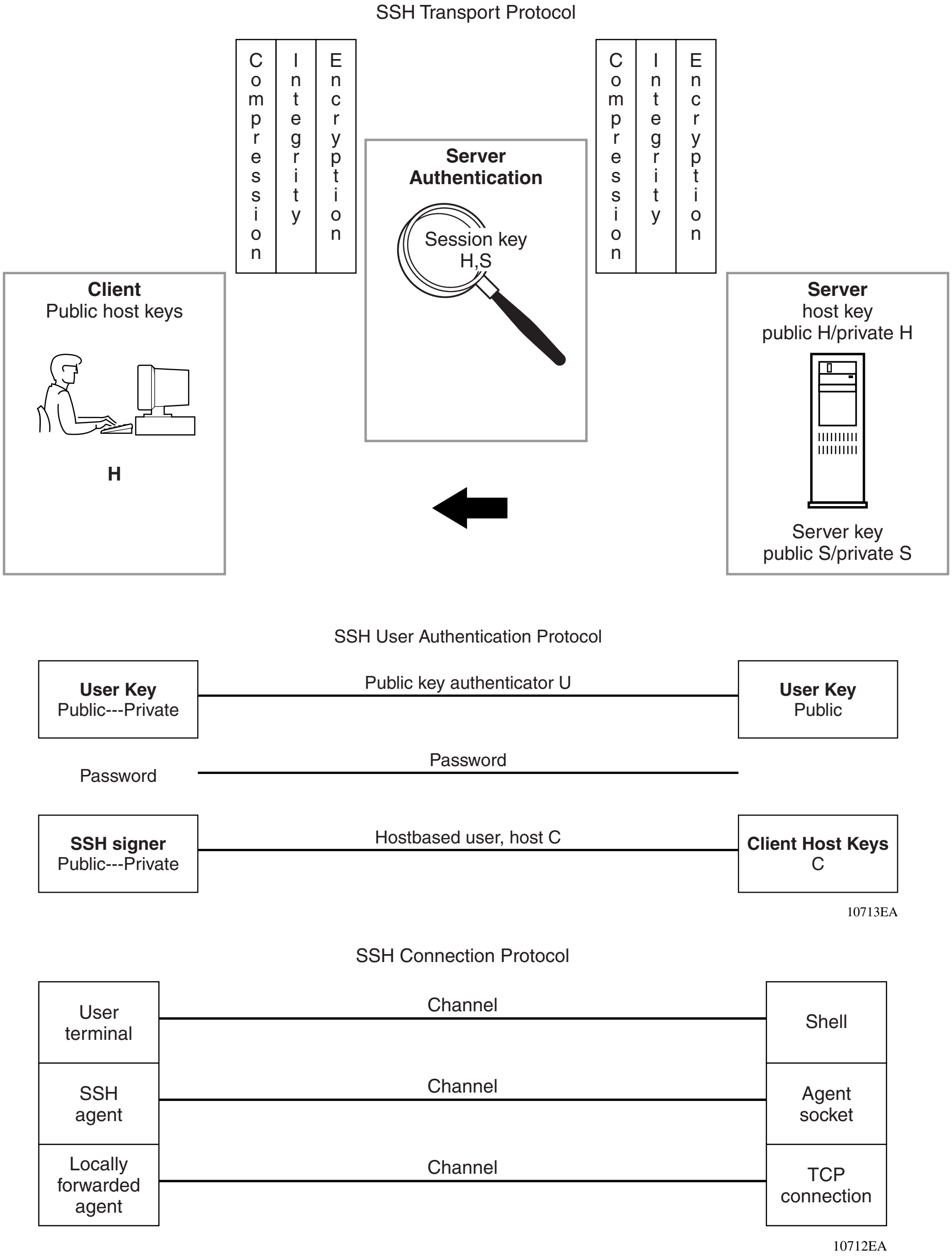
  The SSH authentication protocol runs on top of the SSH transport layer and authenticates the client-side user to the server. SSH-AUTH defines three authentication methods: public key, host-based, and password. SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- SSH Connection Protocol (SSH-CONN)

  The SSH connection protocol runs on top of the SSH transport layer and user authentication protocols. SSH-CONN provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. These richer services are multiplexed into the single encrypted tunnel provided by the SSH transport layer.

Figure 2 shows the three layers of the SSH-2 protocol.

Figure 2 Separate SSH version 2 protocols



The modular approach of SSH-2 improves on the security, performance, and portability of the SSH-1 protocol.

➡ **Note:** The SSH-1 and SSH-2 protocols are not compatible. The SSH implementation on the BayStack 420/425 Switch only supports the more secure version, the SSH-2 protocol. Ensure that your SSH client supports the SSH-2 protocol.

Establishing a secure SSH connection

To establish a secure SSH connection to the BayStack 420/425 Switch:

1 Configure and enable the SSH service on the switch. (Refer to "Configuring SSH using the Nortel Networks Command Line Interface (NNCLI)" on page 18)

➡ **Note:** You must use the NNCLI to initially configure SSH. You can use DM to change the SSH configuration parameters. However, Nortel Networks recommends using the NNCLI.

By default, the SSH service when enabled listens for connections on port 22. It allows up to 2 simultaneous SSH connections. In the default configuration, sessions can be authenticated by either password or public key authentication.

2 Connect to the switch using your SSH client.

Refer to the documentation that came with your selected SSH client for information on initiating a secure SSH connection to the switch.

a To connect to the switch using password authentication:

— Enter either the Console Read-Only switch password (default is *user*) or the Console Read-Write switch password (default is *secure*) when asked to enter the password.

When using password authentication, the user name is not required.

➡ **Note:** Using the Console Read-Only or Console Read-Write password does not set read-only or read-write privileges. Either password will work to establish a secure SSH connection to the device.

b To connect to the switch using DSA public key authentication:

— Generate a DSA key pair (public and private keys) using your SSH client or key-gen tool and export your public key.

Refer to the documentation that came with your selected SSH client or key-gen tool for information on generating a DSA key pair and exporting the public key.

— Download the DSA public key file to the switch via your TFTP server. (Refer to “Configuring SSH using the Nortel Networks Command Line Interface (NNCLI)” on page 18.)

— Connect to the switch using DSA public key authentication.

Please refer to the documentation that came with your SSH client for information on establishing a secure SSH connection using DSA public key authentication.

Configuring SSH using the Nortel Networks Command Line Interface (NNCLI)

This section provides the NNCLI commands for configuring and managing SSH on the BayStack 420/425 Switch. The SSH protocol provides secure access to the NNCLI. With the NNCLI, you use the following commands:

- “show ssh global command,” next
- “show ssh session command” on page 20
- “show ssh download-auth-key command” on page 20
- “ssh dsa-host-key command” on page 21
- “no ssh dsa-host-key command” on page 22
- “ssh command” on page 22
- “no ssh command” on page 22
- “ssh secure command” on page 23
- “ssh timeout command” on page 23
- “ssh dsa-auth command” on page 23
- “no ssh dsa-auth command” on page 24
- “ssh pass-auth command” on page 24
- “no ssh pass-auth command” on page 24
- “ssh port command” on page 24

- "ssh download-auth-key command" on page 25
- "default ssh command" on page 25

show ssh global command

The `show ssh global` command displays the secure shell configuration information. The syntax for the `show ssh global` command is:

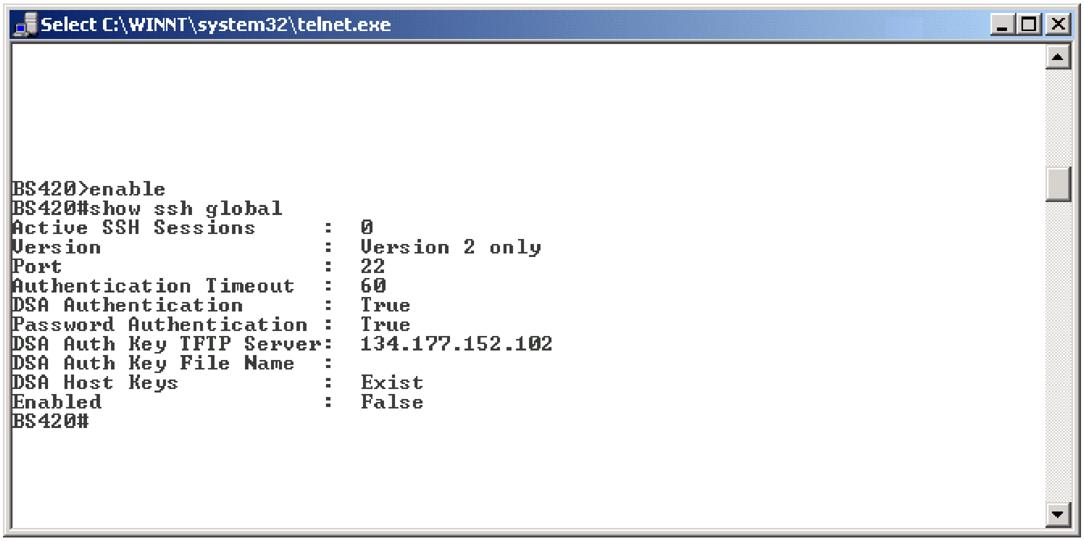
```
show ssh global
```

The `show ssh global` command is in the privExec command mode.

The `show ssh global` command has no parameters or variables.

Figure 3 displays sample output from the `show ssh global` command.

Figure 3 show ssh global command output



```
BS420>enable
BS420#show ssh global
Active SSH Sessions      :  0
Version                  :  Version 2 only
Port                     :  22
Authentication Timeout   :  60
DSA Authentication       :  True
Password Authentication  :  True
DSA Auth Key TFTP Server:  134.177.152.102
DSA Auth Key File Name   :
DSA Host Keys            :  Exist
Enabled                  :  False
BS420#
```

show ssh session command

The show ssh session command displays the SSH session information. The session information includes the session ID and the host IP address. A host address of 0.0.0.0 indicates no connection for that session ID. The syntax for the show ssh session command is:

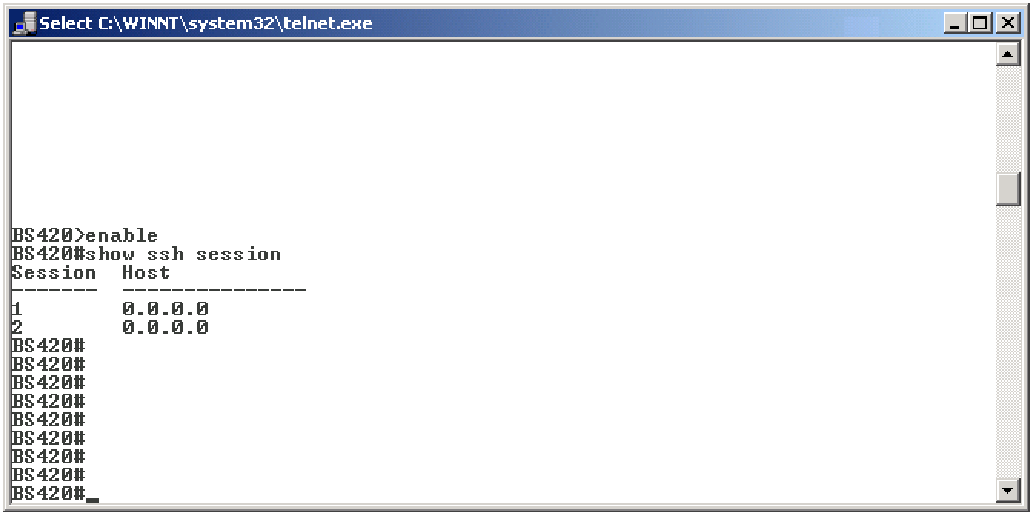
```
show ssh session
```

The show ssh session command is in the privExec command mode.

The show ssh session command has no parameters or variables.

Figure 4 displays sample output from the show ssh session command.

Figure 4 show ssh session command output



Select C:\WINNT\system32\telnet.exe

```
BS420>enable
BS420#show ssh session
Session   Host
-------   ---------------
1         0.0.0.0
2         0.0.0.0
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#_
```

show ssh download-auth-key command

The show ssh download-auth-key command displays the results of the most recent attempt to download the DSA public key from the TFTP server. The syntax for the show ssh download-auth-key command is:

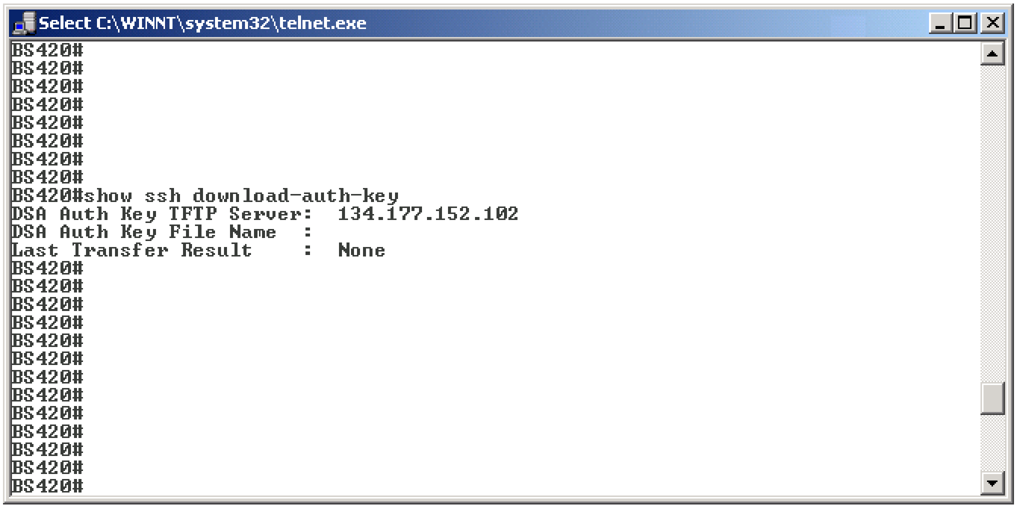
```
show ssh download-auth-key
```

The `show ssh download-auth-key` command is in the privExec command mode.

The `show ssh download-auth-key` command has no parameters or variables.

Figure 5 displays sample output from the `show ssh session` command.

Figure 5 show ssh download-auth-key command output



```
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#show ssh download-auth-key
DSA Auth Key TFTP Server:  134.177.152.102
DSA Auth Key File Name   :
Last Transfer Result     :  None
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
BS420#
```

ssh dsa-host-key command

The `ssh dsa-host-key` command initiates generation of DSA host key at next system reboot. This command can only be executed in SSH disable mode. The syntax of the `ssh dsa-host-key` command is:

```
ssh dsa-host-key
```

The `ssh dsa-host-key` command is in the config command mode.

There are no parameters or variables for the `ssh dsa-host-key` command

no ssh dsa-host-key command

The `no ssh dsa-host-key-gen` command deletes the DSA host key in the switch. The syntax of the `no ssh dsa-host-key-gen` command is:

```
no ssh dsa-host-key
```

The `no ssh dsa-host-key` command is in the config command mode.

There are no parameters or variables for the `no ssh dsa-host-key` command.

ssh command

The `ssh` command enables the SSH server on the BayStack 420/425 Switch in non-secure mode. In addition to accepting SSH connections, the BayStack 420/ 425 Switch continues to accept Web, SNMP, and Telnet connections while in this mode.The syntax of the `ssh` command is:

```
ssh
```

The `ssh` command is in the config command mode.

There are no parameters or variables for the `ssh` command.

no ssh command

The `no ssh` command disables the SSH server on the BayStack 420/425 Switch. The syntax of the `no ssh` command is:

```
no ssh
```

The `no ssh` command is in the config command mode.

There are no parameters or variables for the `no ssh` command.

ssh secure command

The ssh secure command enables the SSH server on the BayStack 420/425 Switch in secure mode. In secure mode, the BayStack 420/425 Switch does not accept Web, SNMP, or Telnet connections. The syntax of the ssh secure command is:

```
ssh secure
```

The ssh secure command is in the config command mode.

There are no parameters or variables for the ssh secure command.

ssh timeout command

The ssh timeout command sets the timeout value for session authentication. The syntax of the ssh timeout command is:

```
ssh timeout <1-120>
```

The ssh timeout command is in the config command mode.

Table 1 describes the parameters and variables for the ssh timeout command.

Table 1 ssh timeout command parameters and variables

Parameters and variables	Description
<1-120>	Specifies the timeout value for authentication. Default is 60.

ssh dsa-auth command

The ssh dsa-auth command enables DSA authentication. The syntax of the ssh dsa-auth command is:

```
ssh dsa-auth
```

The ssh dsa-auth command is in the config command mode.

There are no parameters or variables for the ssh dsa-auth command.

no ssh dsa-auth command

The `no ssh dsa-auth` command disables DSA authentication. The syntax of the `no ssh dsa-auth` command is:

```
no ssh dsa-auth
```

The `no ssh dsa-auth` command is in the config command mode.

There are no parameters or variables for the `no ssh dsa-auth` command.

ssh pass-auth command

The `ssh pass-auth` command enables password authentication. The syntax of the `ssh pass-auth` command is:

```
ssh pass-auth
```

The `ssh pass-auth` command is in the config command mode.

There are no parameters or variables for the `ssh pass-auth` command.

no ssh pass-auth command

The `no ssh pass-auth` command disables password authentication. The syntax of the `no ssh pass-auth` command is:

```
no ssh pass-auth
```

The `no ssh pass-auth` command is in the config command mode.

There are no parameters or variables for the `no ssh pass-auth` command.

ssh port command

The `ssh port` command sets the SSH connection port. The syntax of the `ssh port` command is:

```
ssh port <1-65535>
```

The ssh port command is in the config command mode.

Table 2 describes the parameters and variables for the ssh port command.

Table 2 ssh port command parameters and variables

Parameters and variables	Description
<1-65535>	Specifies the SSH connection port. Default is 22.

ssh download-auth-key command

The ssh download-auth-key command downloads the client public key from the TFTP server to the BayStack 420/425 Switch. The syntax for the ssh download-auth-key is:

```
ssh download-auth-key [address <XXX.XXX.XXX.XXX>] [key-name
<file>]
```

The ssh download-auth-key command is in the config command mode.

Table 3 describes the parameters and variables for the ssh download-auth-key command.

Table 3 ssh download-auth-key command parameters and variables

Parameters and variables	Description
address <XXX.XXX.XXX.XXX>	The IP address of the TFTP server.
key-name <file>	The name of the public key file on the TFTP server.

default ssh command

The default ssh command resets the specific secure shell configuration parameter to the default value. The syntax of the default ssh command is:

```
default ssh [dsa-auth|pass-auth|port|timeout]
```

The default ssh command is in the config command mode.

Table 4 describes the parameters and variables for the `default ssh` command.

Table 4 default ssh command parameters and variables

Parameters and variables	Description
dsa-auth	Resets dsa-auth to the default value. Default is True.
pass-auth	Resets pass-auth to the default value. Default is True.
port	Resets the port number for SSH connections to the default. Default is 22.
timeout	Resets the timeout value for session authentication to the default. Default is 60.

Distributed Multilink Trunking (DMLT)

Distributed Multilink Trunking (DMLT) on the BayStack 425 switch allows trunked ports to span multiple units within the same stack configuration to provide fail-safe connectivity. This configuration is called a *distributed trunk.*

Distributed MultiLink Trunks allow you to group up to four switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices (up to 800 Mb/s in full-duplex mode).

You can configure up to six MultiLink Trunks. MultiLink Trunking software detects misconfigured (or broken) trunk links and redirects traffic on the misconfigured or broken trunk link to other trunk members within that trunk.

You can use the Trunk Configuration screen with the CI menus, the Web-based management system, the CLI, or DM to create switch-to-switch and switch-to-server MultiLink Trunk links.

How the MultiLink Trunk reacts to losing distributed trunk members

At present, if your distributed MultiLink Trunk spans two or more units in a stack configuration, and any one of the units becomes inactive from a loss of power or a unit failure, the entire stack becomes inactive, and the distributed multilink trunk is lost.

In the case of a stack failure, until the stack recovers, all ports in MLT and DMLT are in a partition state and will not allow an ingress or egress state. This avoids a potential loop being introduced for the failed stack.

If a stack recovers on its own, the MLT and DMLT will return to their normal state. If not, you must reset the stack.

EAPOL-based security

BayStack 420/425 Switch software version 3.0 provides support for security based on the Extensible Authentication Protocol over LAN (EAPOL), which uses the EAP as described in the IEEE Draft P802.1X to allow you to set up network access control on internal LANs.

EAP allows the exchange of authentication information between any end station or server connected to the switch and an authentication server (such as a RADIUS server). The EAPOL-based security feature operates in conjunction with a RADIUS-based server to extend the benefits of remote authentication to internal LAN clients.

The following example illustrates how the BayStack 425, configured with the EAPOL-based security feature, reacts to a new network connection:

- The switch detects a new connection on one of its ports.
  - The switch requests a user ID from the new client.
  - EAPOL encapsulates the user ID and forwards it to the RADIUS server.
  - The RADIUS server responds with a request for the user’s password.
- The new client forwards an encrypted password to the switch, within the EAPOL packet.
  - The switch relays the EAPOL packet to the RADIUS server.
  - If the RADIUS server validates the password, the new client is allowed access to the switch and the network.

Some components and terms used with EAPOL-based security are:

- Supplicant—the device applying for access to the network.

- Authenticator—software with the sole purpose of authorizing a supplicant that is attached to the other end of a LAN segment.
- Authentication Server—a RADIUS server that provides authorization services to the Authenticator.
- Port Access Entity (PAE)—a software entity associated with each port that supports the Authenticator or Supplicant functionality. In the preceding example, the Authenticator PAE resides on the switch.
- Controlled Port—any switch port with EAPOL-based security enabled.

The Authenticator communicates with the Supplicant using an encapsulation mechanism known as EAP over LANs (EAPOL).

The Authenticator PAE encapsulates the EAP message into a RADIUS packet before sending the packet to the Authentication Server. The Authenticator facilitates the authentication exchanges that occur between the Supplicant and the Authentication Server by encapsulating the EAP message to make it suitable for the packet's destination.

The Authenticator determines the controlled port's operational state. After the RADIUS server notifies the Authenticator PAE about the success or failure of the authentication, it changes the controlled port's operational state accordingly.

The Authenticator PAE functionality is implemented for each controlled port on the switch. At system initialization, or when a supplicant is initially connected to the switch's controlled port, the controlled port's state is set to Blocking. During that time, EAP packets are processed by the authenticator.

When the Authentication server returns a "success" or "failure" message, the controlled port's state is changed accordingly. If the authorization is successful, the controlled port's operational state is set to Forwarding. Otherwise, the controlled port's state depends on the Operational Traffic Control field value in the EAPOL Security Configuration screen.

The Operational Traffic Control field can have one of the following two values:

- Incoming and Outgoing—If the controlled port is unauthorized, frames are not transmitted through the port; all frames received on the controlled port are discarded. The controlled port's state is set to Blocking.
- Incoming—If the controlled port is unauthorized, frames received on the port are discarded, but the transmit frames are forwarded through the port.

EAPOL dynamic VLAN assignment

If EAPOL-based security is enabled on a port, and then the port is authorized, the EAPOL feature dynamically changes the port's VLAN configuration according to preconfigured values, and assigns a new VLAN. The new VLAN configuration values are applied according to previously stored parameters (based on the user_id) in the Authentication server.

The following VLAN configuration values are affected:

- Port membership
- PVID
- Port priority

When the EAPOL-based security is disabled on a port that was previously authorized, the port's VLAN configuration values are restored directly from the switch's non-volatile random access memory (NVRAM).

The following exceptions apply to dynamic VLAN assignments:

- The dynamic VLAN configuration values assigned by EAPOL are **not** stored in the switch's NVRAM.
- You can override the dynamic VLAN configuration values assigned by EAPOL; however, be aware that the values you configure are not stored in NVRAM.
- When EAPOL is enabled on a port, and you configure values other than VLAN configuration values, those values are applied and stored in NVRAM.

You set up your Authentication server (RADIUS server) for EAPOL dynamic VLAN assignments. The Authentication server allows you to configure user-specific settings for VLAN memberships and port priority.

When you log on to a system that has been configured for EAPOL authentication, the Authentication server recognizes your user ID and notifies the switch to assign preconfigured (user-specific) VLAN membership and port priorities to the switch. The configuration settings are based on configuration parameters that were customized for your user ID and previously stored on the Authentication server.

To set up the Authentication server, set the following “Return List” attributes for all user configurations (refer to your Authentication server documentation):

- VLAN membership attributes
  - Tunnel-Type: value 13, Tunnel-Type-VLAN
  - Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
  - Tunnel-Private-Group-Id: ASCII value 1 to 4094 (this value is used to identify the specified VLAN)
- Port priority (vendor-specific) attributes
  - Vendor Id: value 562, Nortel Networks vendor Id
  - Attribute Number: value 1, Port Priority
  - Attribute Value: value 0 (zero) to 7 (this value is used to indicate the port priority value assigned to the specified user)

System requirements

The following are minimum system requirements for the EAPOL-based security feature:

- At least one of the following supported switches:
  - BayStack 350/410-24T/450 switch (software version V4.0, or later)
  - BayStack 425-24T (software version V3.0, or later)
- RADIUS server (Microsoft Windows .NET Server)
- Client software that supports EAPOL (Microsoft Windows XP Client)

You must specify the Microsoft 2001 IAS server (or any generic RADIUS server that supports EAP) as the primary RADIUS server for these devices. You must also configure your BayStack 350/410-24T/450 switches and BayStack 425 for port-based VLANs and EAPOL security.

EAPOL-based security configuration rules

The following configuration rules apply to your BayStack 425-24T when using EAPOL-based security:

- Before configuring your switch, you must configure the Primary RADIUS Server and Shared Secret fields.

- You cannot configure EAPOL-based security on ports that are currently configured for:
  - MultiLink Trunking
  - MAC address-based security
  - IGMP (Static Router Ports)
  - Port mirroring
- You can connect only a single client on each port that is configured for EAPOL-based security. (If you attempt to add additional ports to a port, that port goes to Blocking mode.)

EAPOL-based security uses the RADIUS protocol to authenticate local console, Telnet, and EAPOL-authorized logins.

RADIUS-based network security

The RADIUS-based security feature allows you to set up network access control, using the Remote Authentication Dial-In User Services (RADIUS) security protocol. The RADIUS-based security feature uses the RADIUS protocol to authenticate local console and Telnet logins.

You will need to set up specific user accounts (user names and passwords, and Service-Type attributes) on your RADIUS server before the authentication process can be initiated. To provide each user with appropriate levels of access to the switch, set the following username attributes on your RADIUS server:

- Read-write access—Set the Service-Type field value to Administrative.
- Read-only access—Set the Service-Type field value to NAS-Prompt.

For detailed instructions to set up your RADIUS server, refer to your RADIUS server documentation.

Configuring EAPOL using Device Manager

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access control protocol. EAPoL provides security to your network by preventing users from accessing network resources before they are authenticated.

EAPoL allows you to set up network access control on internal LANs and to exchange authentication information between any end station or server connected to the BayStack 425 switch and an authentication server (such as a RADIUS server). This security feature extends the benefits of remote authentication to internal LAN clients. For example, if a new client PC fails the authentication process, EAPoL prevents it from accessing the network.

Configuration prerequisites

Use the following configuration rules when using EAPoL:

- Before configuring your switch, you must configure at least one EAPoL RADIUS Server and Shared Secret fields.
- You cannot configure EAPoL on ports that are currently configured for:
  - MultiLink Trunking
  - MAC address-based security
  - IGMP (Static Router Ports)
  - Port mirroring
- Before you globally enable EAPoL on the switch, change the AuthControlledPortControl field to *auto* for each port that you want **controlled**. The *auto* setting automatically authenticates the port according to the results of the RADIUS server. The default authentication setting for each port is *forceAuthorized*.
- You can connect only a single client on each port that is configured for EAPoL. (If you attempt to add additional ports to a port, that port goes to Blocking mode.)

EAPoL uses the RADIUS protocol to authenticate local console, Telnet, and EAPoL-authorized logins.

EAPOL tab for a single port

The EAPOL tab allows you to configure EAPOL-based security for a single port.

To view the EAPOL tab:

1 Select the port you want to edit.

2 Do one of the following:

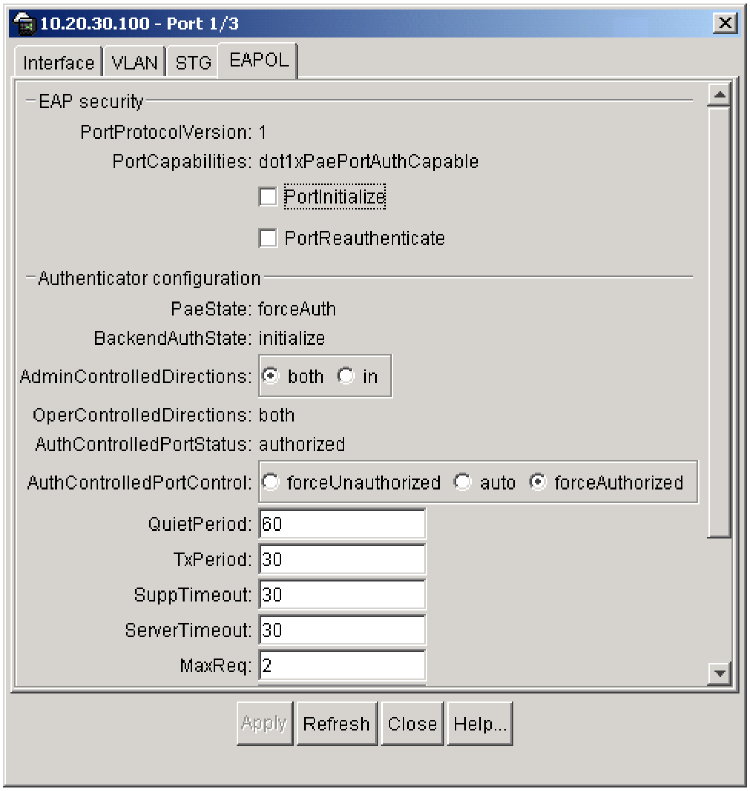
- Double-click the selected port
- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for a single port opens with the Interface tab displayed.

3 Click the EAPOL tab.

The EAPOL tab opens (Figure 6).

Figure 6 Edit Port dialog box — EAPOL tab



EAP security

PortProtocolVersion: 1

PortCapabilities: dot1xPaePortAuthCapable

□ PortInitialize

□ PortReauthenticate

Authenticator configuration

PaeState: forceAuth

BackendAuthState: initialize

AdminControlledDirections: ● both ○ in

OperControlledDirections: both

AuthControlledPortStatus: authorized

AuthControlledPortControl: ○ forceUnauthorized ○ auto ● forceAuthorized

QuietPeriod: 60

TxPeriod: 30

SuppTimeout: 30

ServerTimeout: 30

MaxReq: 2

Table 5 describes the EAPOL tab items.

Table 5 EAPOL tab items for a single port

Item	Description
PortProtocolVersion	The EAP Protocol version that is running on this port.
PortCapabilities	The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Setting this attribute to True causes this port's EAPOL state to be initialized.
PortReauthenticate	Setting this attribute to True causes the reauthentication of the client.
PaeState	The current authenticator PAE state machine stat value.
BackendAuthState	The current state of the Backend Authentication state machine.
AdminControlledDirections	The current value of the administrative controlled directions parameter for the port.
OperControlledDirections	The current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	The current value of the controlled port status parameter for the port.
AuthControlledPortControl	The current value of the controlled port control parameter for the port.
QuietPeriod	The current value of the time interval between authentication failure and the start of a new authentication.
TxPeriod	Time to wait for response from supplicant for EAP requests/ Identity packets.
SuppTimeout	Time to wait for response from supplicant for all EAP packets except EAP Request/Identity.
ServerTimeout	Time to wait for a response from the RADIUS server
MaxReq	Number of times to retry sending packets to the supplicant.
ReAuthPeriod	Time interval between successive re-authentications.
ReAuthEnabled	Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field.
KeyTxEnabled	The value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant.

Table 5 EAPOL tab items for a single port (continued)

Item	Description
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

Viewing and editing multiple port configurations

To view or edit the configurations of multiple ports:

1 Select the ports you want to edit.

Press [Ctrl] + left click the ports you want to view or configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- Double-click on the selected port.
- On the toolbar, click Edit.

Note: When you edit multiple ports, some tabs are not available, and some tabs are available even though the options are not applicable. When the option does not apply for a given port, NoSuchObject is displayed.

EAPOL Diag tab for graphing ports

The EAPOL Diag tab displays EAPOL diagnostics statistics.

To open the EAPOL Diag tab for graphing:

1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

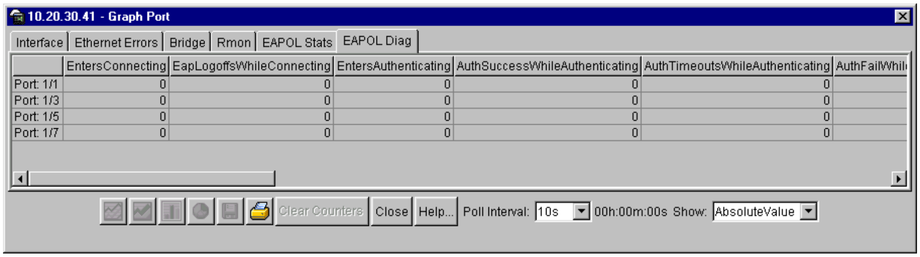
- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3 Click the EAPOL Diag tab.

The EAPOL Diag tab for graphing multiple ports opens (Figure 7).

Figure 7 Graph Port dialog box — EAPOL Diag tab


10.20.30.41 - Graph Port

	EntersConnecting	EapLogoffsWhileConnecting	EntersAuthenticating	AuthSuccessWhileAuthenticating	AuthTimeoutsWhileAuthenticating	AuthFailWhil
Port: 1/1	0	0	0	0	0	
Port: 1/3	0	0	0	0	0	
Port: 1/5	0	0	0	0	0	
Port: 1/7	0	0	0	0	0	

Poll Interval: 10s 00h:00m:00s Show: AbsoluteValue

Table 6 describes the EAPOL Diag tab fields.

Table 6 EAPOL Diag tab fields

Field	**Description**
EntersConnecting	Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/Identity message being received from the supplicant.
AuthSuccessWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the supplicant.
AuthTimeoutsWhile Authenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout.
AuthFailWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure.
AuthReauthsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of a reauthentication request.

Table 6 EAPOL Diag tab fields (continued)

Field	Description
AuthEapStartsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Logoff message being received from the supplicant.
AuthReauthsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Disconnected as a result of an EAPOL-Logoff message being received from the supplicant.
BackendResponses	Counts the number of times that the Backend Authentication state machine sends an Initial-Access request packet to the Authentication server.
BackendAccessChallenges	Counts the number of times that the Backend Authentication state machine receives an Initial-Access challenge packet from the Authentication server.
BackendOtherRequestsToSupplicant	Counts the number of times that the Backend Authentication state machine sends an EAP request packet (other than an Identity, Notification, failure, or success message) to the supplicant.
BackendNonNakResponsesFromSupplicant	Counts the number of times that the Backend Authentication state machine receives a response from the supplicant to an initial EAP request and the response is something other than EAP-NAK.
BackendAuthSuccesses	Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server.
BackendAuthFails	Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server.

Configuring EAPOL using NNCLI

You configure the security based on the Extensible Authentication Protocol over LAN (EAPOL) using the following NNCLI commands:

- "show eapol command," next
- "eapol command" on page 39
- "eapol command for modifying parameters" on page 40

show eapol command

The `show eapol` command displays the status of the EAPOL-based security. The syntax for the `show eapol` command is:

```
show eapol
```

The `show eapol` command is in the privExec command mode.

The `show eapol` command has no parameters or variables.

The `show eapol` command displays the current status of the EAPOL parameters.

eapol command

The `eapol` command enables or disables EAPOL-based security. The syntax of the `eapol` command is:

```
eapol {disable|enable}
```

The `eapol` command is in the config command mode.

Table 7 describes the parameters and variables for the `eapol` command.

Table 7 eapol command parameters and variables

Parameters and variables	Description
disable|enable	Disables or enables EAPOL-based security.

eapol command for modifying parameters

The eapol command for modifying parameters modifies EAPOL-based security parameters for a specific port. The syntax of the eapol command for modifying parameters is:

```
eapol [port <portlist>] [init] [status
authorized|unauthorized|auto] [traffic-control in-out|in]
[re-authentication enable|disable]
[re-authentication-interval <num>]
[re-authentication-period <1-604800>] [re-authenticate]
[quiet-interval <num>] [transmit-interval <num>]
[supplicant-timeout <num>] [server-timeout
<num>][max-request <num>]
```

The eapol command for modifying parameters is in the config-if command mode.

Table 8 describes the parameters and variables for the eapol command for modifying parameters

Table 8 eapol command for modifying parameters and variables

Parameters and variables	Description
port <portllist>	Specifies the ports to configure for EAPOL; enter the port numbers you want. Note: If you omit this parameter, the system uses the port number specified when you issued the interface command.
init	Re-initiates EAP authentication.

Table 8 eapol command for modifying parameters and variables

Parameters and variables	Description
status authorized|unauthorized|auto	Specifies the EAP status of the port: • authorized—port is always authorized • unauthorized—port is always unauthorized • auto—port authorization status depends on the result of the EAP authentication
traffic-control in-out|in	Sets the level of traffic control: • in-out—if EAP authentication fails, both ingressing and egressing traffic are blocked • in—if EAP authentication fails, only ingressing traffic is blocked
re-authentication enable|disable	Enables or disables re-authentication.
re-authentication-interval <num>	Enter the number of seconds you want between re-authentication attempts; range is 1 to 604800. Use either this variable or the re-authentication-period variable; do not use both variables because the two variables control the same setting.
re-authentication-period <1-604800>	Enter the number of seconds you want between re-authentication attempts. Use either this variable or the re-authentication-interval variable; do not use both variables because the two variables control the same setting.
re-authenticate	Specifies an immediate re-authentication.
quiet-interval <num>	Enter the number of seconds you want between an authentication failure and the start of a new authentication attempt; range is 1 to 65535.
transmit-interval <num>	Specifies a waiting period for response from supplicant for EAP Request/Identity packets. Enter the number of seconds you want to wait; range is 1-65535.
supplicant-timeout <num>	Specifies a waiting period for response from supplicant for all EAP packets except EAP Request/Identity packets. Enter the number of seconds you want to wait; range is 1-65535.
server-timeout <num>	Specifies a waiting period for response from the server. Enter the number of seconds you want to wait; range is 1-65535
max-request <num>	Enter the number of times to retry sending packets to supplicant.

Using RADIUS authentication

Using a the RADIUS protocol and a server, you can configure the BayStack 420/425 Switch for authentication. With the CLI system, you use the following commands:

- “show radius-server command,” next
- “radius-server command” on page 42
- “no radius-server command” on page 43

show radius-server command

The `show radius-server` command displays the RADIUS server configuration. The syntax for the `show radius-server` command is:

```
show radius-server
```

The `show radius-server` command is in the privExec command mode.

The `show radius-server` command has no parameters or variables.

Figure 8 displays sample output from the `show radius-server` command.

Figure 8 show radius-server command output

```
BS425_24#show radius-server
host: 0.0.0.0
Secondary-host: 0.0.0.0
port: 1645
key:
BS425_24#
```

radius-server command

The `radius-server` command changes the RADIUS server settings. The syntax for the `radius-server` command is:

```
radius-server host <address> [secondary-host <address>] port
<num> key <string>
```

The `radius-server` command is in the config command mode.

Table 9 describes the parameters and variables for the `radius-server` command.

Table 9 radius-server command parameters and variables

Parameters and variables	Description
host <address>	Specifies the primary RADIUS server. Enter the IP address of the RADIUS server.
secondary-host <address>	Specifies the secondary RADIUS server Enter the IP address of the secondary RADIUS server.
port <num>	Enter the port number of the RADIUS server.
key <string>	Specifies a secret text string that is shared between the switch and the RADIUS server. Enter the secret string, which is an alphanumeric string up to 16 characters.

no radius-server command

The `no radius-server` command clears the RADIUS server settings. The syntax for the `no radius-server` command is:

```
no radius-server
```

The `no radius-server` command is in the config command mode.

The `no radius-server` command has no parameters or values.

Configuring EAPOL using the Console Interface

The EAPOL Security Configuration screen in the Console Interface allows you to selectively limit access to the switch based on an authentication mechanism that uses Extensible Authentication Protocol (EAP) to exchange authentication information between the switch and an authentication server.

Note: Before you use the EAPOL Security Configuration screen, you must configure your Primary RADIUS Server and RADIUS Shared Secret.

You will also need to set up specific user accounts on your RADIUS server:

- User names
- Passwords
- VLAN IDs (optional)
- Port priority (optional)

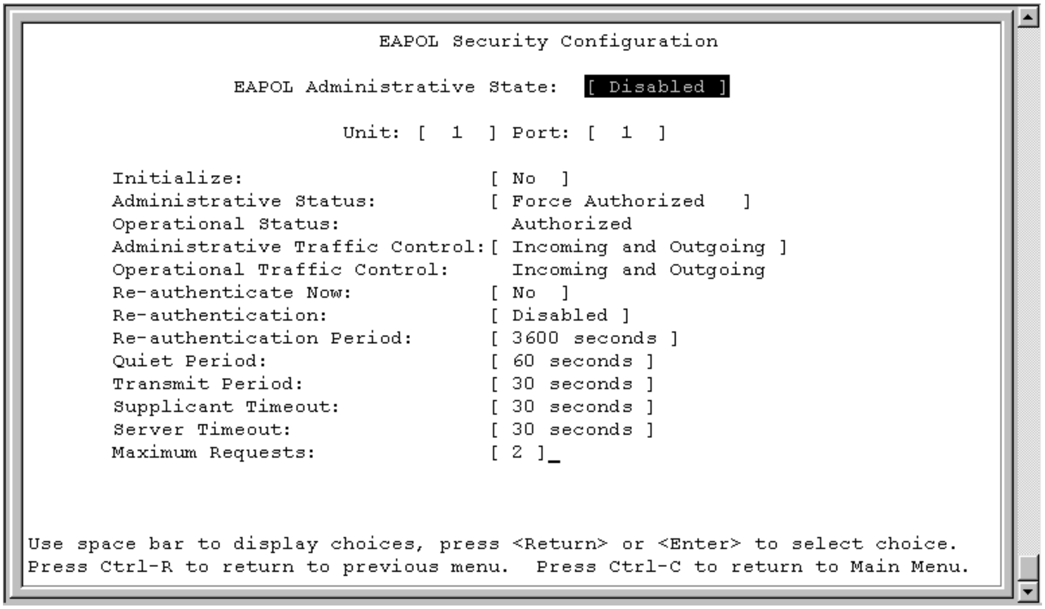
You can set up these parameters directly on your RADIUS server. For detailed instructions about configuring your RADIUS server, refer to your RADIUS server documentation.

Note: Do not enable EAPOL security on the switch port that is connected to the RADIUS server.

To open the EAPOL Security Configuration screen:

Ë Choose EAPOL Security Configuration (or press e) from the Switch Configuration Menu.

Figure 9 EAPOL Security Configuration screen



```
                        EAPOL Security Configuration

             EAPOL Administrative State:  [ Disabled ]

                       Unit: [  1  ] Port: [  1  ]

       Initialize:                     [ No  ]
       Administrative Status:          [ Force Authorized   ]
       Operational Status:               Authorized
       Administrative Traffic Control:[ Incoming and Outgoing ]
       Operational Traffic Control:      Incoming and Outgoing
       Re-authenticate Now:            [ No  ]
       Re-authentication:              [ Disabled ]
       Re-authentication Period:       [ 3600 seconds ]
       Quiet Period:                   [ 60 seconds ]
       Transmit Period:                [ 30 seconds ]
       Supplicant Timeout:             [ 30 seconds ]
       Server Timeout:                 [ 30 seconds ]
       Maximum Requests:               [ 2 ]_



Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 10 describes the EAPOL Security Configuration screen options.

Table 10 EAPOL security configuration screen options

Option	Description
EAPOL Administrative State	Allows you to enable or disable EAPOL for your switch or stack. When this field is set to disabled (the default state), the Operational Status for all of the switch/stack ports is set to Authorized (no security restriction). Default Disabled Range Disabled, Enabled
Unit	Allows you to select the unit number (when stacking is configured) to view or configure. To view or configure another unit, type its unit number and press [Enter], or press the spacebar to toggle the unit numbers. If you set this field value to All, other screen field values you modify apply to *all* stack ports. Default 1 Range 1,2,3,4,5,6,7,8,ALL
Port	Allows you to select a specified unit's (see preceding Unit field) port number to view or configure. To view or configure another port, type its port number and press [Enter], or press the spacebar to toggle the port numbers. If you set this field value to All, other screen field values you modify apply to *all* ports for the specified unit. The All value is also useful when you want to apply modified field values to most of, but not all of, your switch's ports. For example, if you want to apply modified field values to 25 of your switch's 26 ports, it may be easier to apply the All value in the Port field, and then reconfigure the single port back to its original values. Default 1 Range 1 to 26, ALL
Initialize	Allows you to activate EAPOL authentication for the specified unit/port. Default No Range No,Yes
Administrative Status	Allows you to set the EAPOL authorization status for the specified unit/port. Default Force Authorized Range Force Authorized,Force Unauthorized,Auto

Table 10 EAPOL security configuration screen options (continued)

Option	Description
	• Force Authorized means the specified unit/port authorization status is *always* authorized. • Force Unauthorized means the specified unit/port authorization status is *always* Unauthorized. • Auto means the specified unit/port authorization status depends on the EAP authentication results.
Operational Status	A read-only field that shows the current authorization status for the specified unit/port. This read-only field does not appear when the Unit/Port field value is set to All. Default Authorized Range Authorized,Unauthorized
Administrative Traffic Control	Allows you to choose whether EAPOL authentication is set for incoming and outgoing traffic or for incoming traffic only. For example, if you set the specified unit/port field value to Incoming and Outgoing, and the EAPOL authentication fails, then both incoming and outgoing traffic on the specified unit/port is blocked. Default Incoming and Outgoing Range Incoming and Outgoing,Incoming Only
Operational Traffic Control	A read-only field that indicates the current administrative traffic control configuration for the specified unit/port (see preceding field description). This read-only field does not appear when the Unit/Port field value is set to All. Default Incoming and Outgoing Range Incoming and Outgoing,Incoming Only
Re-authenticate Now	Allows you to activate EAPOL authentication for the specified unit/port immediately, without waiting for the Re-Authentication Period to expire. Default No Range No,Yes
Re-authentication	Allows you to repeat EAPOL authentication for the specified unit/port according to the time interval value configured in the Re-Authentication Period field (see next field description). Default Enabled Range Enabled,Disabled
Re-authentication Period	When the Re-Authentication field value (see preceding field) is set to enabled, this field allows you to specify the time period between successive EAPOL authentications for the specified unit/port. Default 3600 seconds Range 1 to 604800 seconds

Table 10 EAPOL security configuration screen options (continued)

Option	Description
Quiet Period	Allows you to specify the time period between any single EAPOL authentication failure and the start of a new EAPOL authentication attempt. Default 60 seconds Range 0 to 65535 seconds
Transmit Period	Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets. Default 30 seconds Range 1 to 65535 seconds
Supplicant Timeout	Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets. Default 30 seconds Range 1 to 65535 seconds
Server Timeout	Allows you to specify how long the switch waits for the RADIUS server to respond to all EAP packets. Default 30 seconds Range 1 to 65535 seconds
Maximum Requests	Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant. Default 2 attempts Range 1 to 10 attempts

ASCII configuration upload and download

This feature uploads or downloads an ASCII configuration file from a TFTP server, parses the commands in the file, and configures the switch based on the commands in the file.

You can edit the configuration file on any host computer using a regular text editor. This provides quick configuration of the switch, using an easy-to-modify text configuration file.

You use the Nortel Networks Command Line Interface (NNCLI) to make changes to the ASCII configuration file.

ASCII Configuration Upload

An ASCII configuration upload from a BayStack 420 or 425 switch to a TFTP server can only be done using CLI commands.

To upload an ASCII configuration in the CLI:

1 Enter the command `copy running-config tftp` with the address of the TFTP server and the filename where you want to store the configuration on the TFTP server.

For example:

```
BS425_24#copy running-config tftp address
100.100.100.2 filename bs425.cfg
```

The system displays the following messages:

```
%Contacting TFTP host: 100.100.100.2

%Generating ASCII configuration: bs425.cfg
```

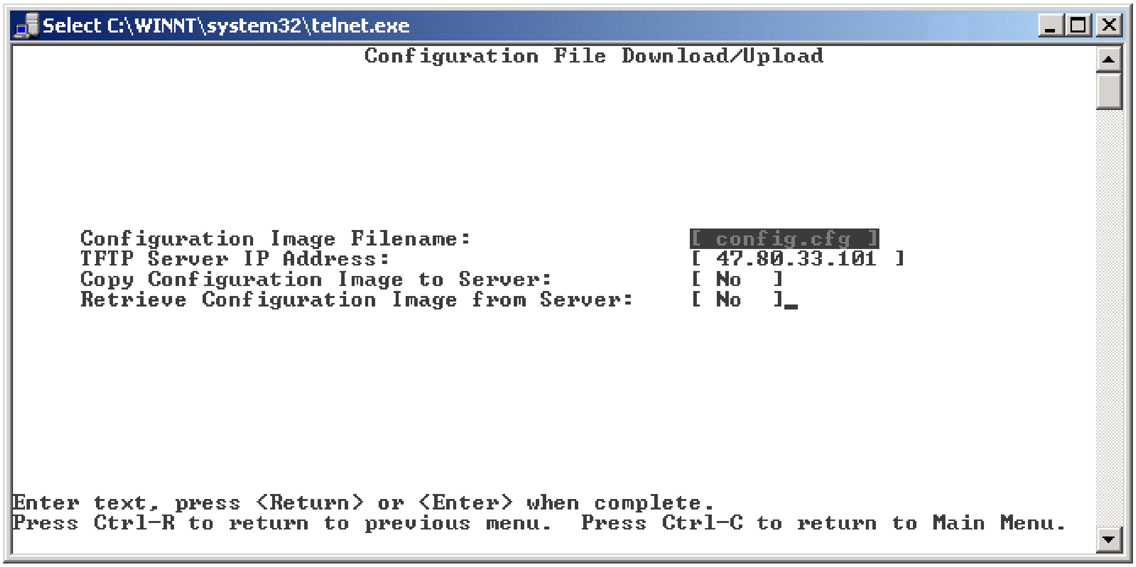
ASCII Configuration File Download screen

The ASCII Configuration File Download screen (Figure 10) allows you to specify the IP address of an TFTP server and the name of the configuration file on the server, and to download an ASCII configuration file containing CLI commands from the TFTP server to configure the switch.

1 Choose ASCII Configuration File Download from the Configuration File.

The Menu opens to the ASCII Configuration File Upload/Download screen.

Figure 10 ASCII Configuration File Upload/Download screen



```
                          Configuration File Download/Upload




     Configuration Image Filename:                [ config.cfg ]
     TFTP Server IP Address:                      [ 47.80.33.101 ]
     Copy Configuration Image to Server:          [ No   ]
     Retrieve Configuration Image from Server:    [ No   ]_




Enter text, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 11 describes the ASCII Configuration File Download screen fields.

Table 11 ASCII Configuration File Download screen fields

Field	Description
Configuration Image Filename	Enter the file name you have chosen for the ASCII configuration file. Choose a meaningful file name that will allow you to identify the file for retrieval when required. The file must already exist on your TFTP server and must be read enabled. Default Value Zero-length string Range An ASCII string of up to 30 printable characters
TFTP Server IP Address	The IP address of your TFTP load host. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Copy Cofiguration Image to server	The IP address of your TFTP load host. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Retrieve Configuration Image from Server	Specifies whether to retrieve the stored switch ASCII configuration file from the specified TFTP server (default is No). If you choose Yes, the download process begins immediately and, when completed, causes the switch to be configured according to the CLI commands in the file. Use the spacebar to toggle the selection to Yes. Press [Enter] to initiate the process. Default Value No Range Yes, No

The ASCII configuration file does not generate any output to the Console. If there is an error in the configuration file, the NNCLI parser exits on the first error found and displays an error message. When you select the 'Yes' option in the 'Retrieve Configuration File from Server' menu item, the file is transferred in ASCII format from the server, via TFTP, and stored in local memory.

When the switch is powered up, there is a delay while the system initializes, resolves its IP address, and spanning tree states go into forwarding, before the switch attempts to retrieve the configuration file. Appropriate messages are displayed during initialization.