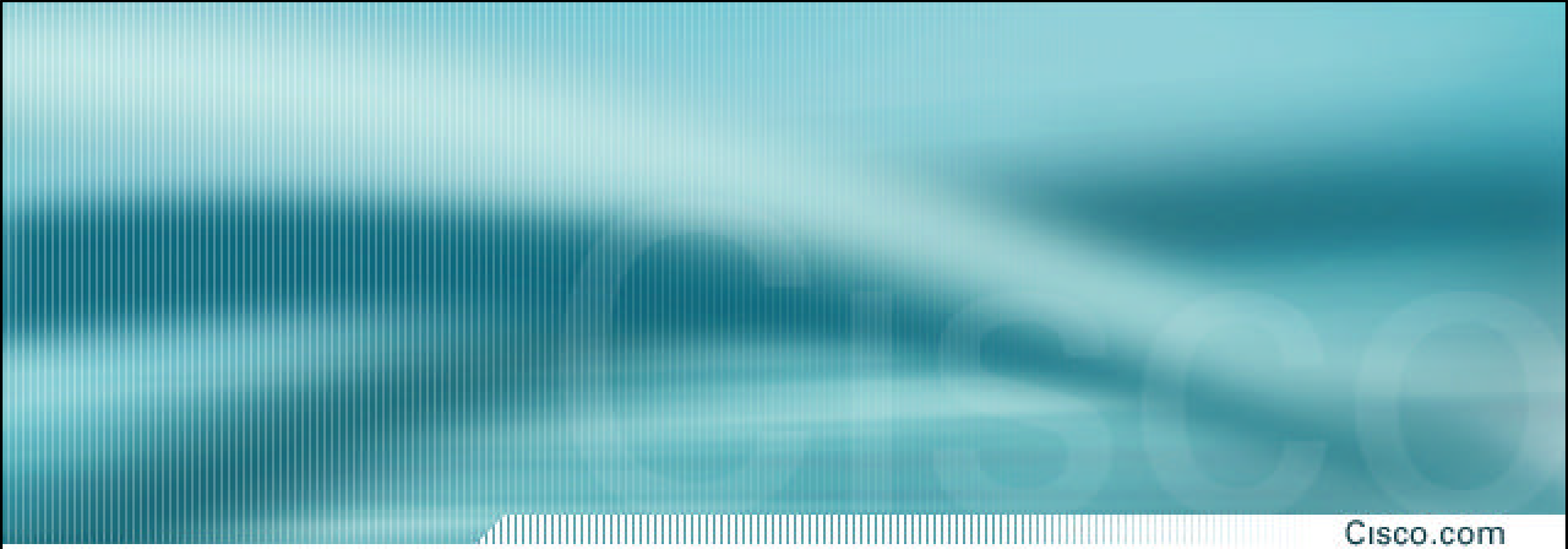


IDS 4.0 Roadshow

Module 3- Sensor Setup

Agenda

Sensor Appliances

Sensor Initialization

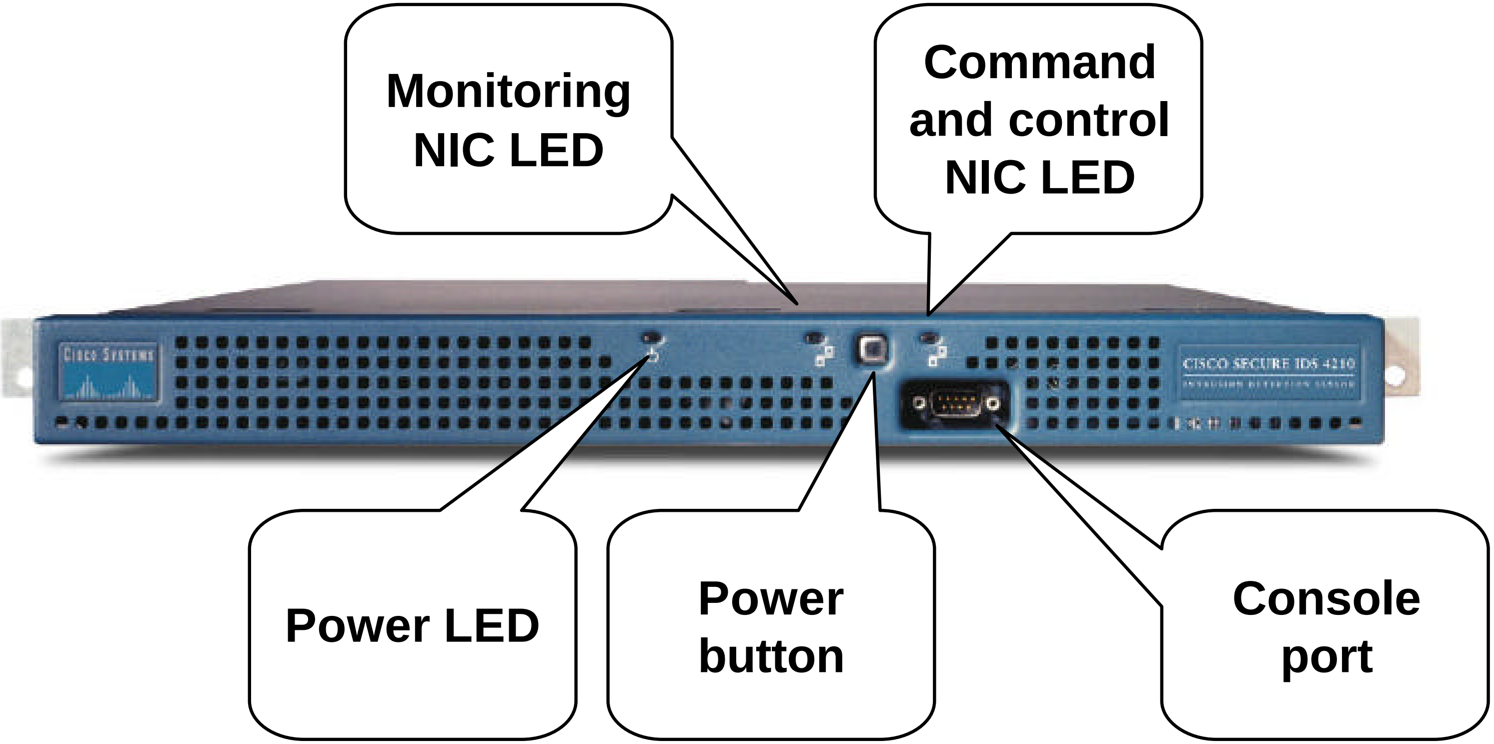
Command Line Modes

Initial Configuration Tasks

Troubleshooting

Sensor Appliances

4210 Sensor Front Panel



Monitoring NIC LED

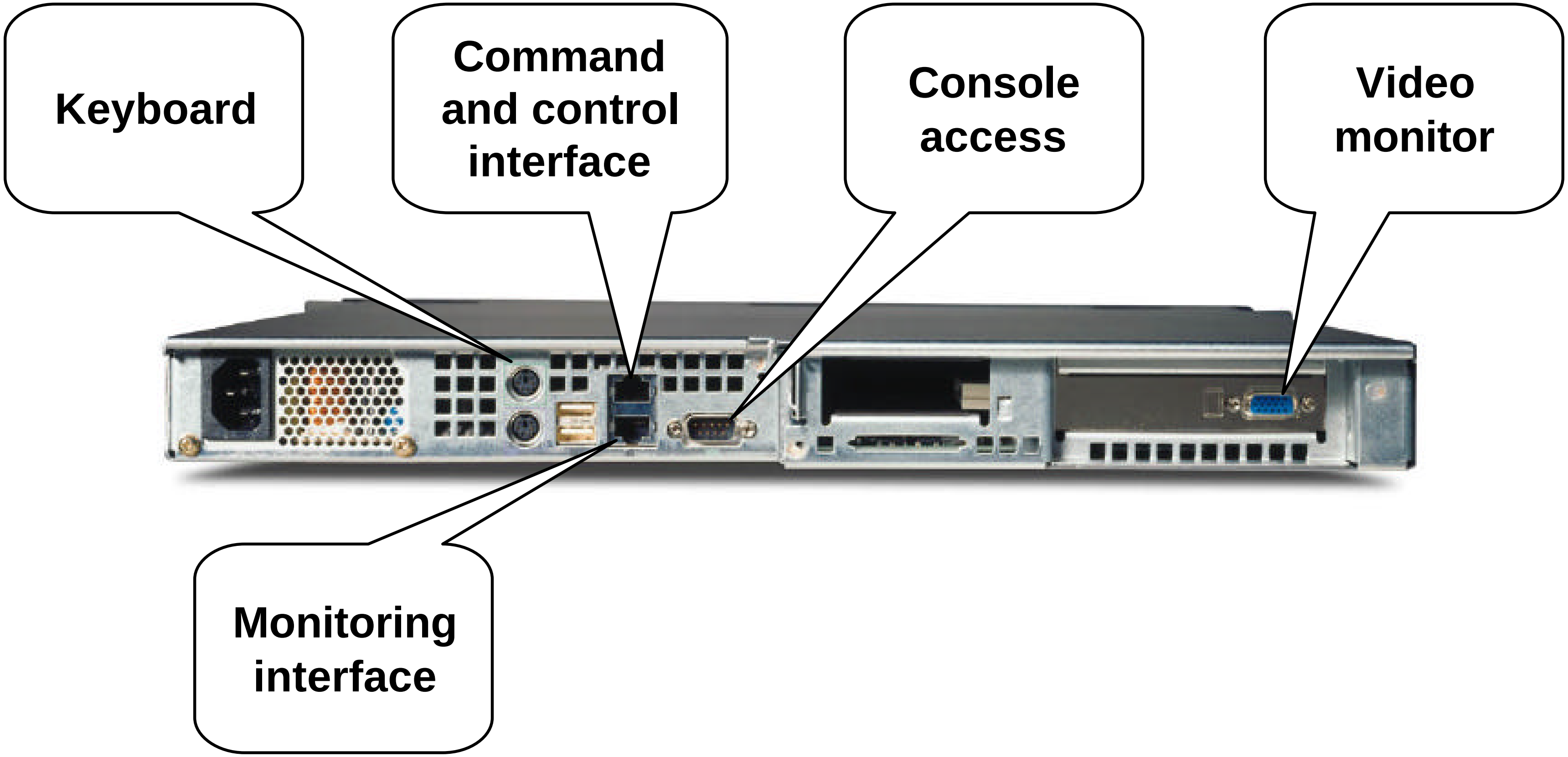
Command and control NIC LED

Power LED

Power button

Console port

4210 Sensor Back Panel



Keyboard

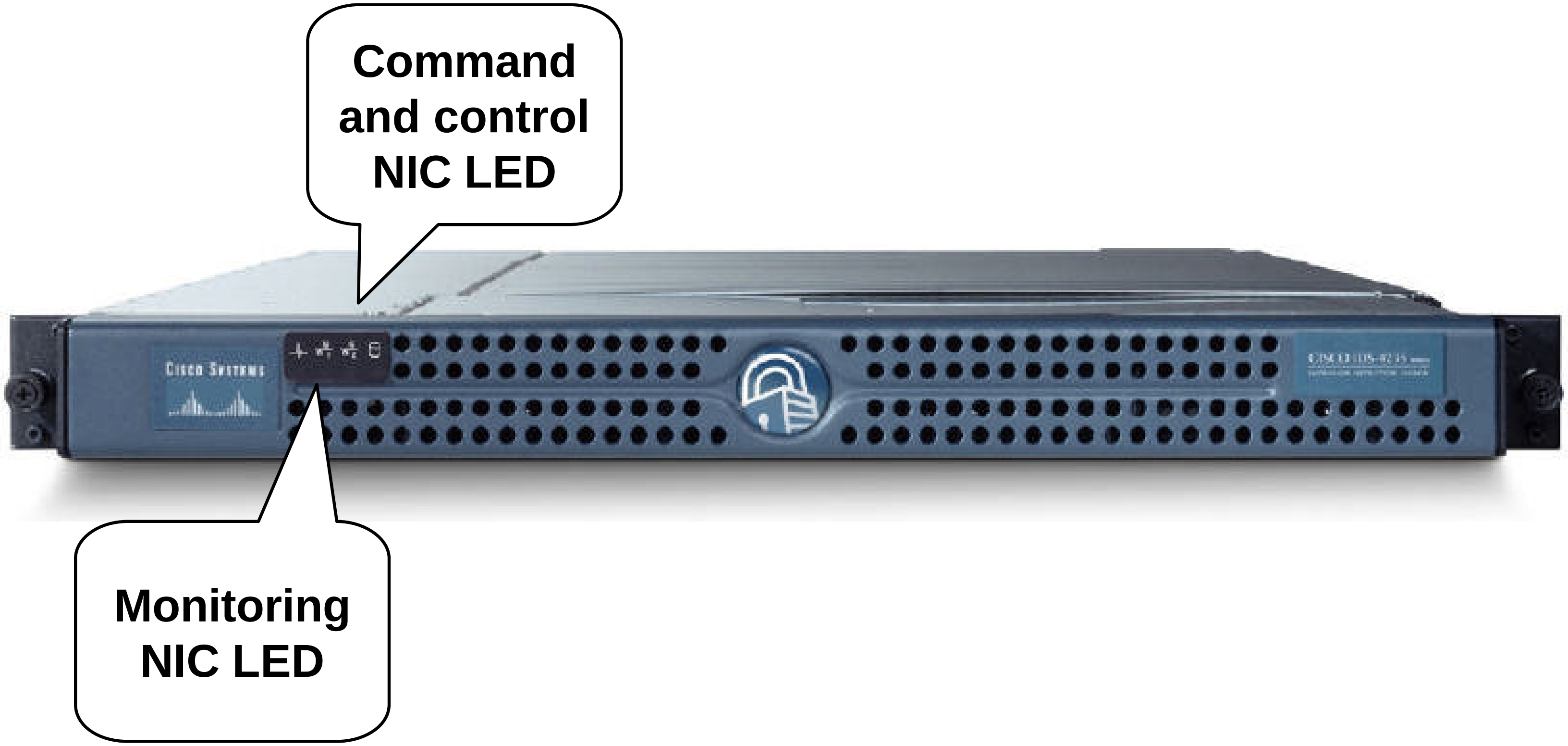
Command and control interface

Console access

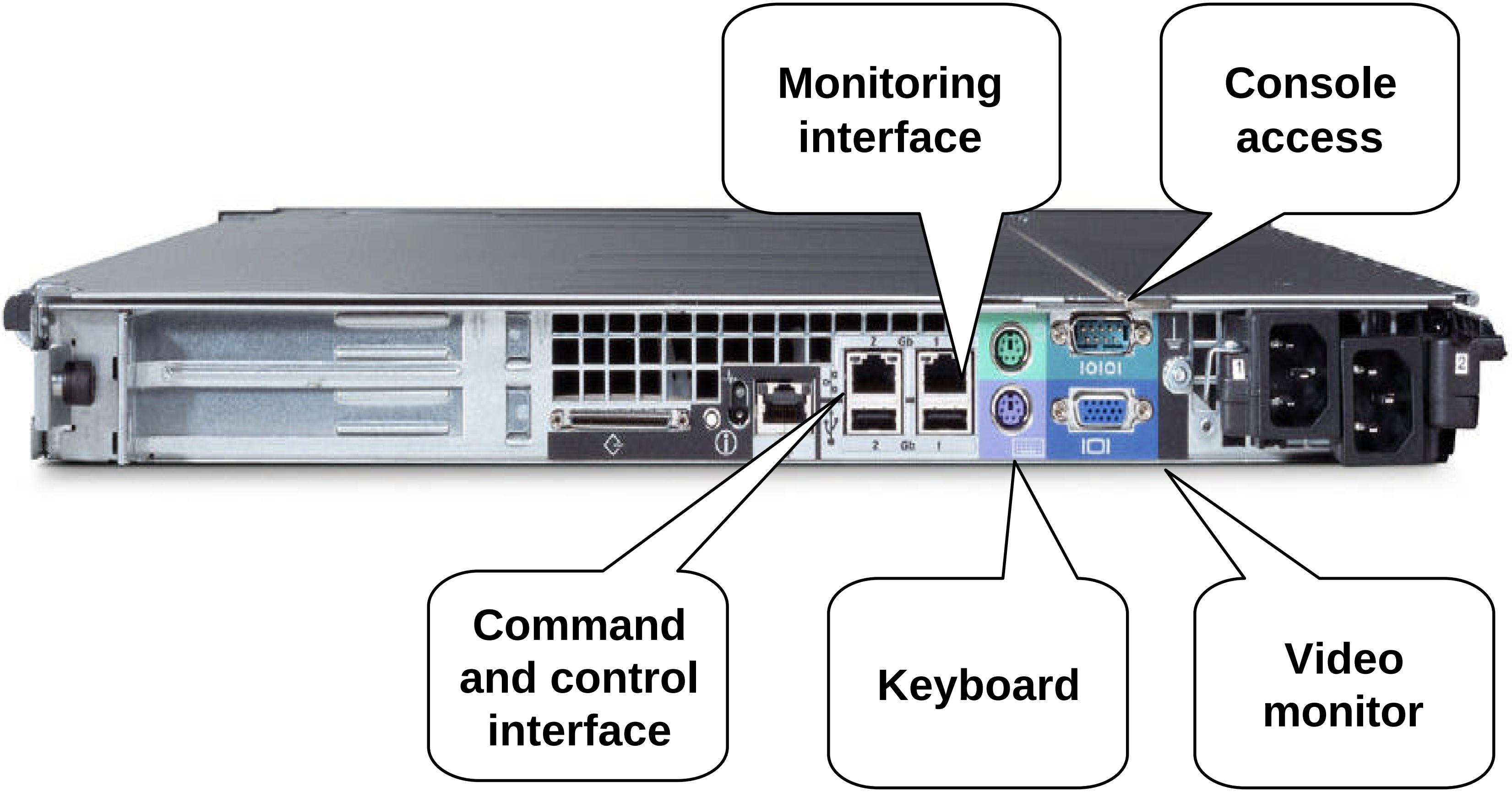
Video monitor

Monitoring interface

4235 Sensor Front Panel



4235 Sensor Back Panel



Monitoring interface

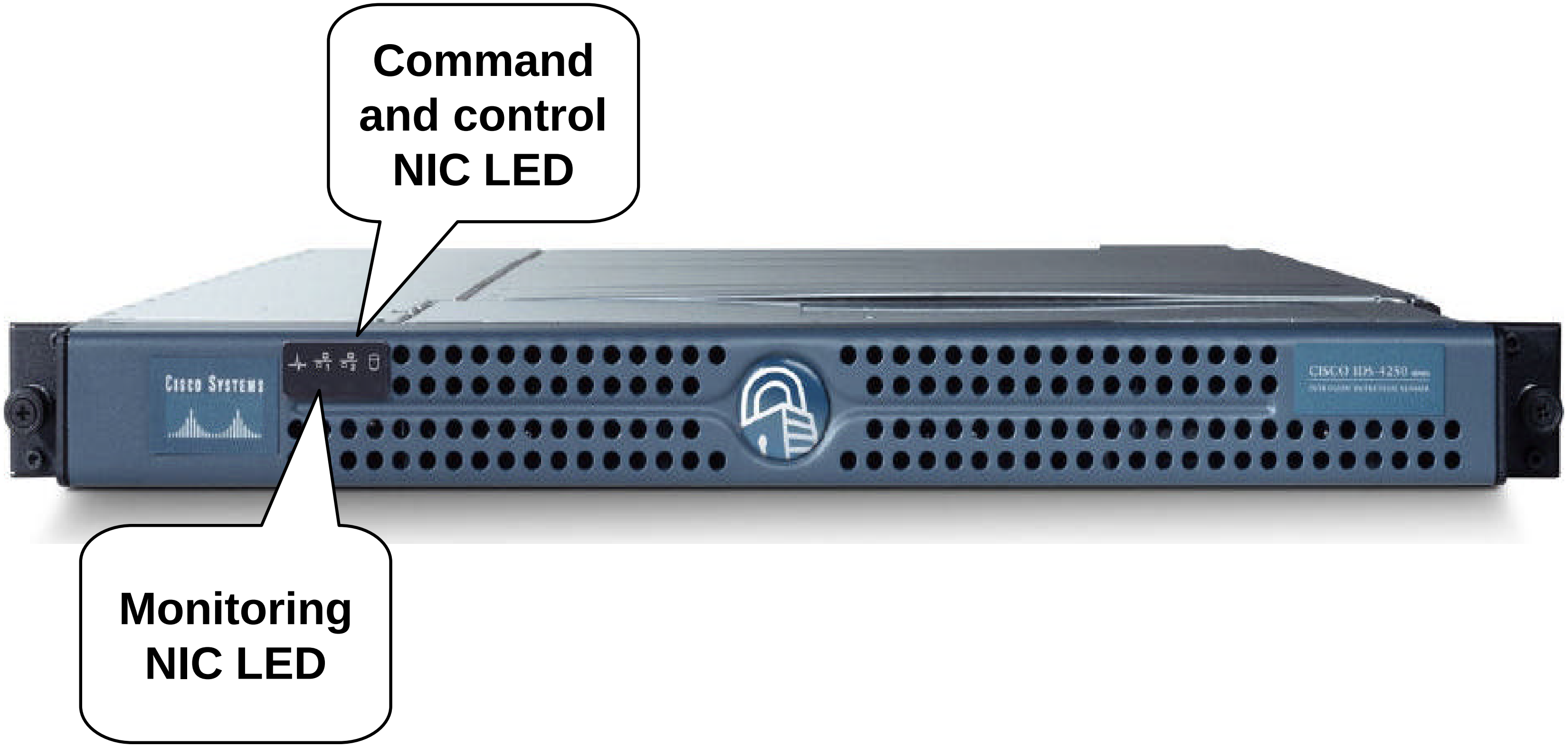
Console access

Command and control interface

Keyboard

Video monitor

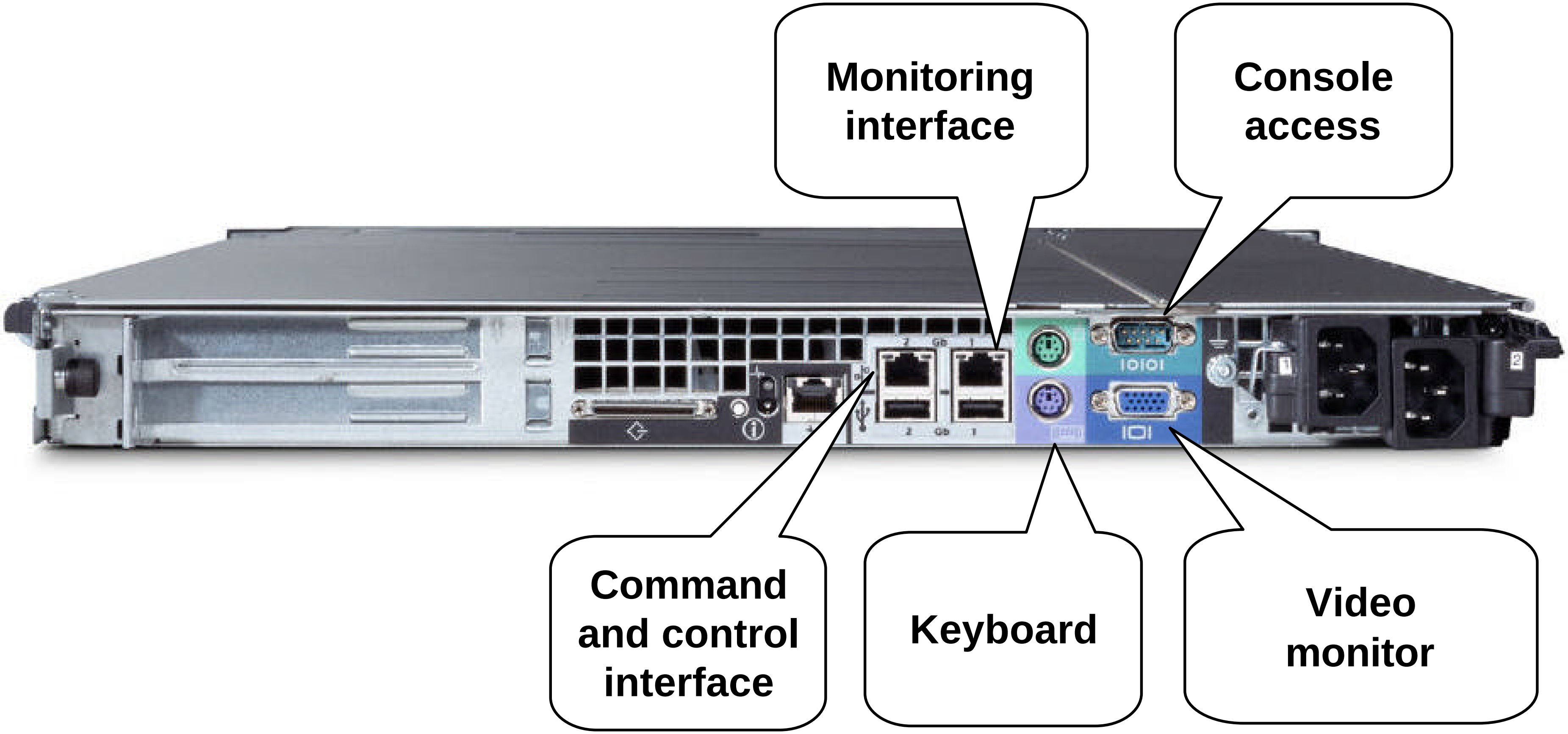
4250 Sensor Front Panel



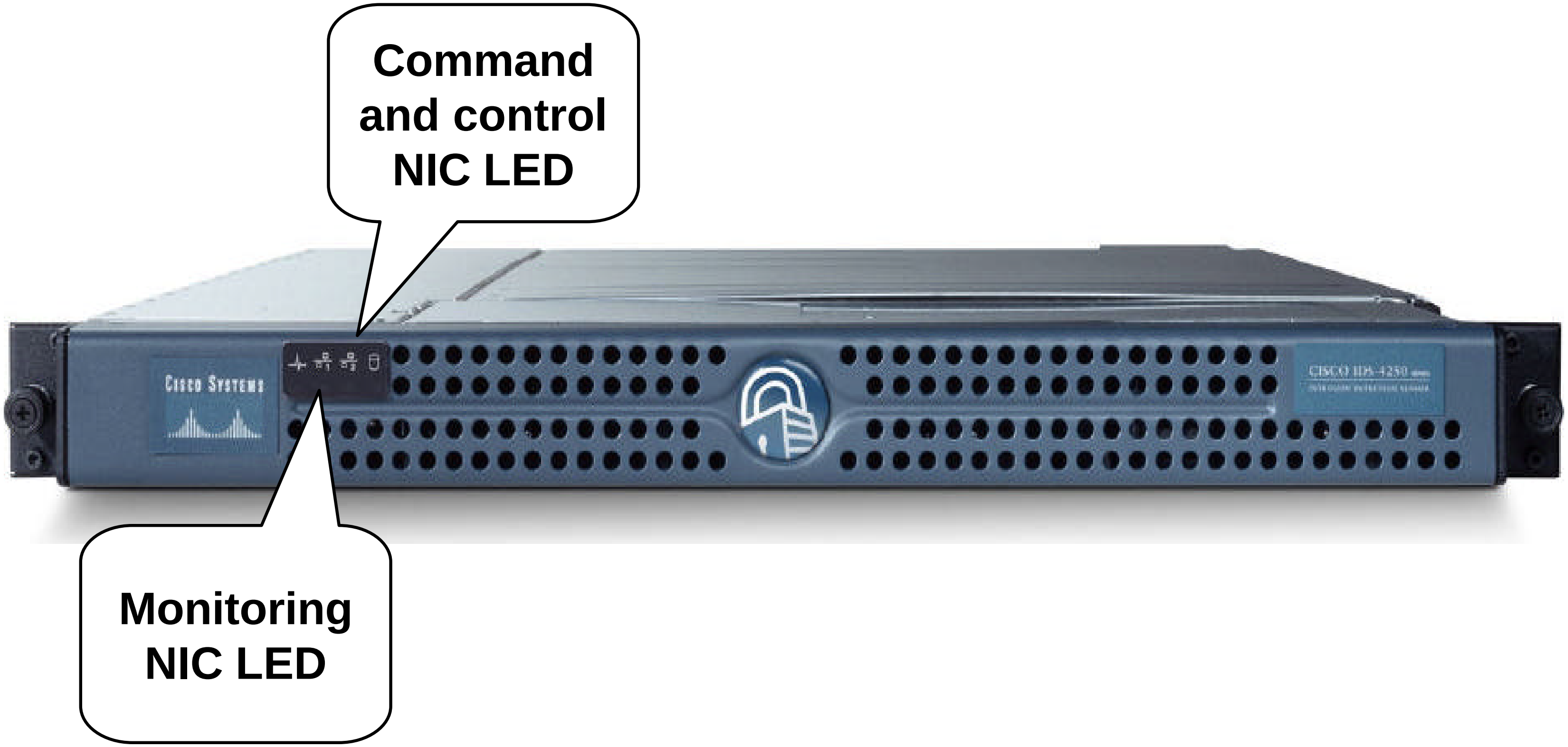
Command and control NIC LED

Monitoring NIC LED

4250 Sensor Back Panel



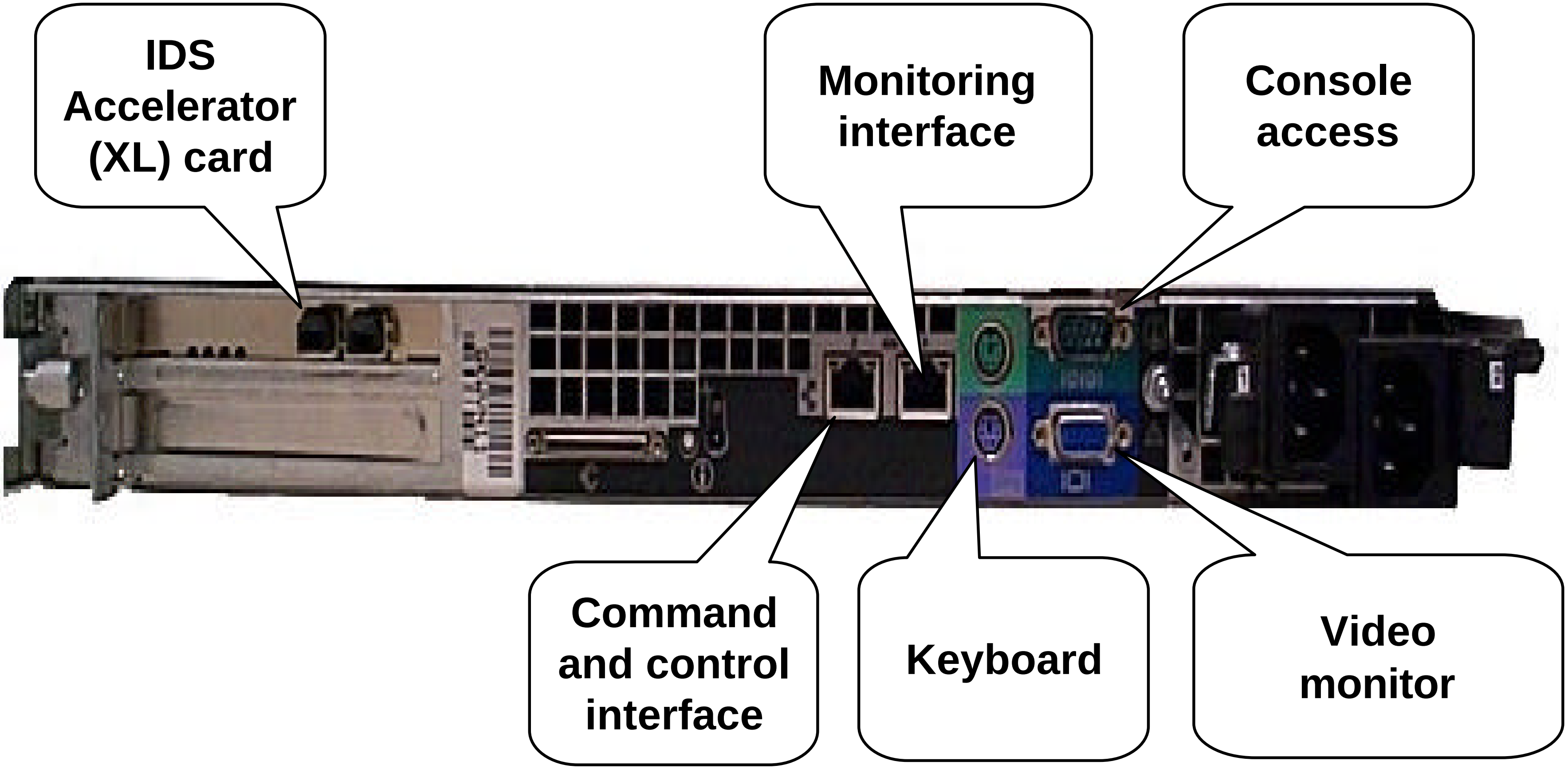
4250-XL Sensor Front Panel



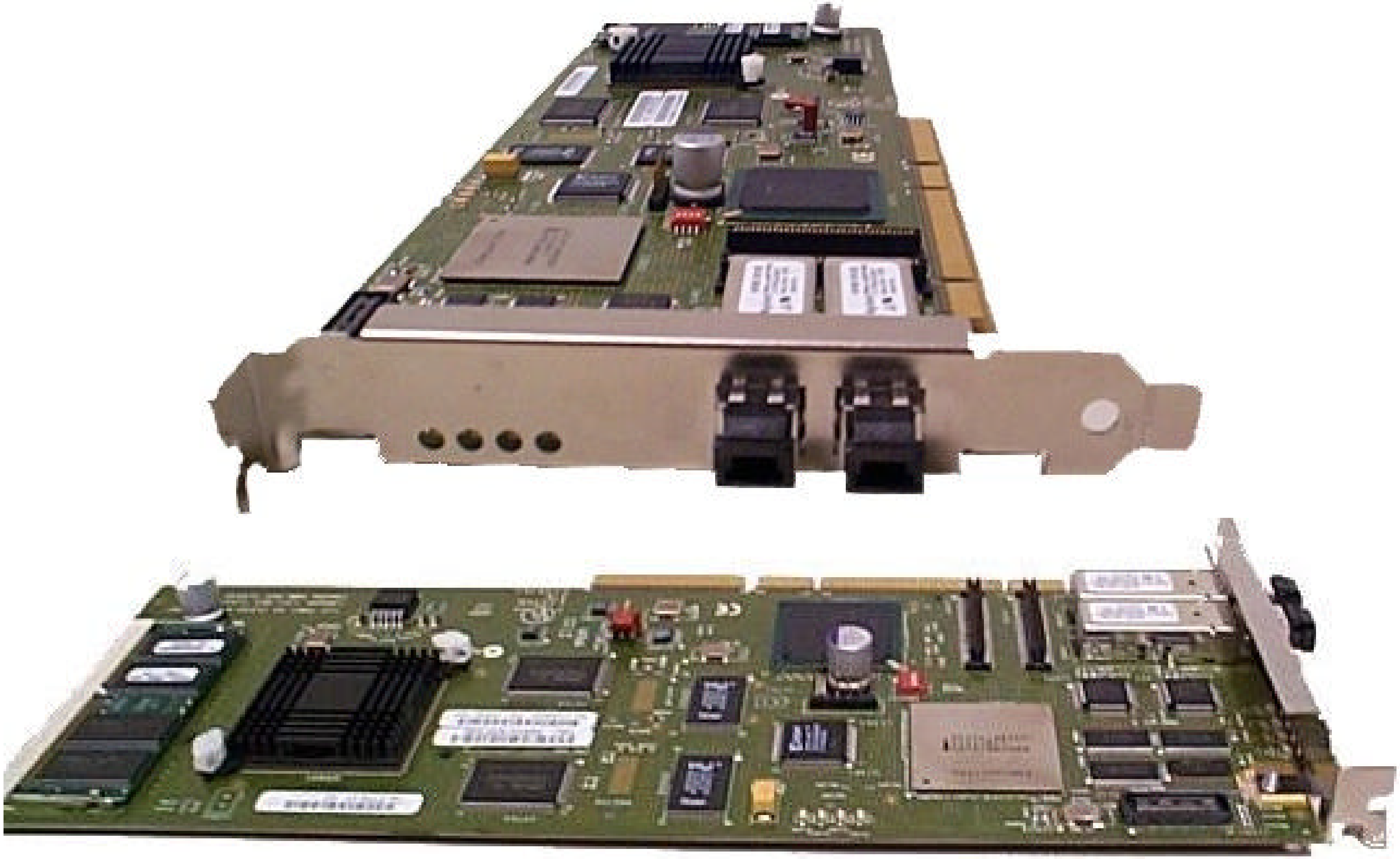
Command and control NIC LED

Monitoring NIC LED

4250-XL Sensor Back Panel



IDS Accelerator (XL) card



Sensor Initialization

Management Access

Following are the methods used to gain management access to a Sensor:

- Console port (cable provided)
- Monitor and keyboard
- Telnet
- SSH
- TLS/SSL

Sensor Login Accounts

User accounts

- Used to access Sensor for management and monitoring
  - via CLI
  - via management consoles
- Created on Sensor
  - via CLI
  - via management consoles
- Default user is cisco with password cisco
- Password change required at first login
- Have roles that determine user's privileges

Service account

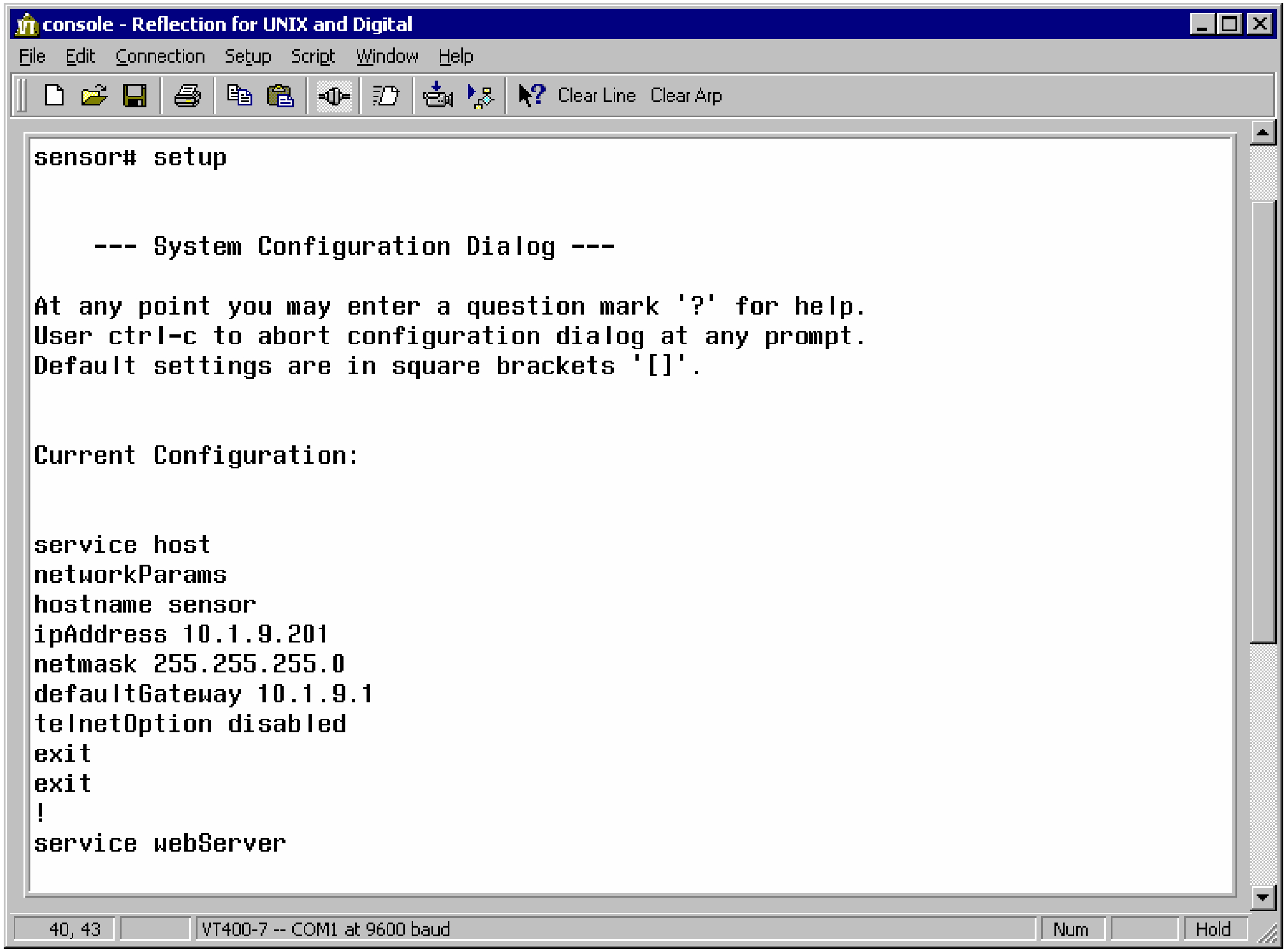
- Special user account that provides root access
- Should be used only for troubleshooting and recovery under direction of TAC
- Does not exist by default
- Can only be used by one user
- Has service role
- Cannot be used remotely

Sensor Initialization Tasks

The following are the tasks to initialize the Sensor:

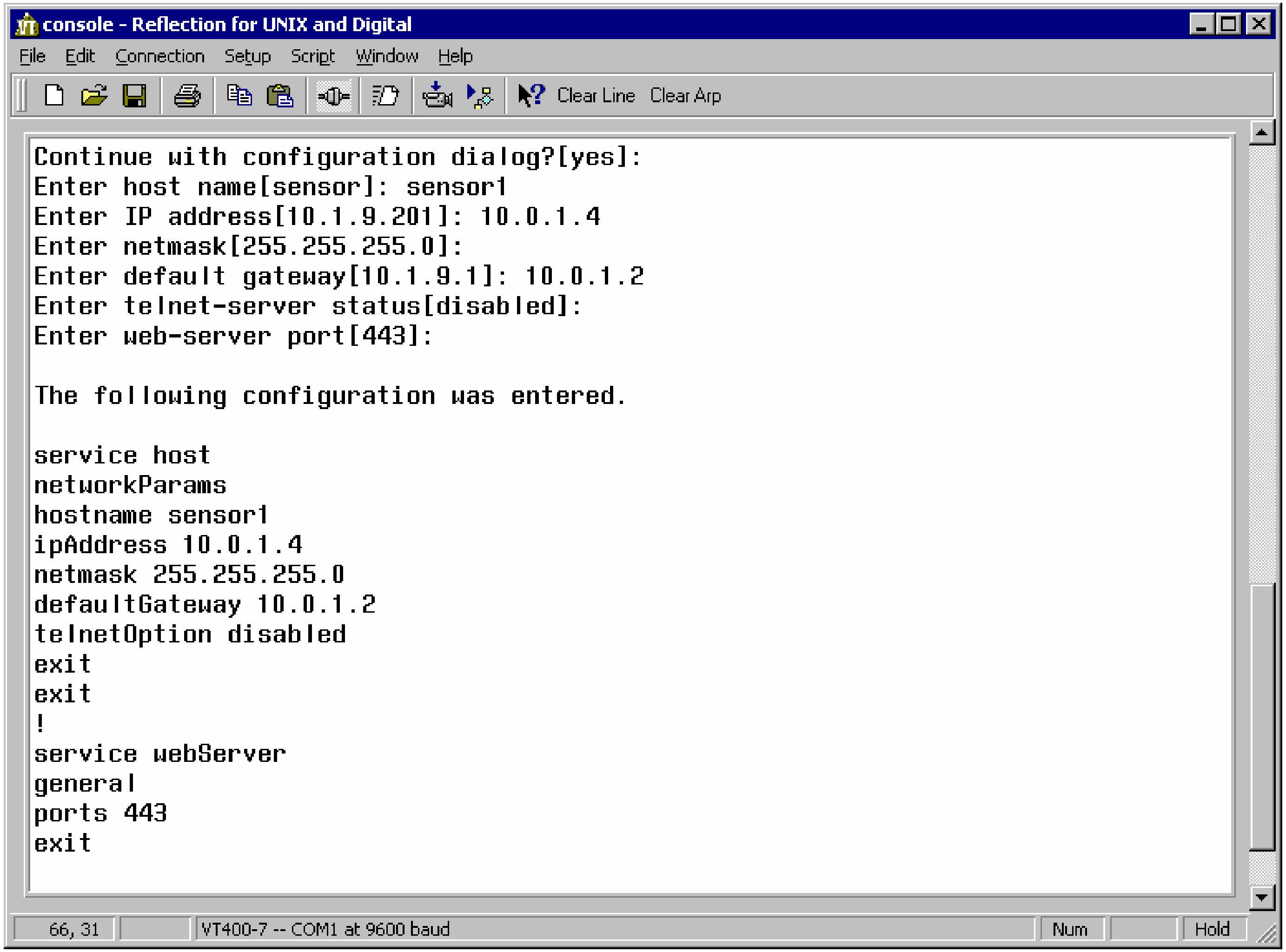
- Assign a name to the Sensor.
- Assign an IP address and netmask to the Sensor's command and control interface.
- Assign a default gateway.
- Enable or disable the Telnet-server.
- Specify the web server port.
- Create network access lists.
- Set the time.
- Generate a self-signed X.509 certificate needed by TLS.
- Create a service account.

setup **Command**


console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
Clear Line Clear Arp
40, 43
VT400-7 -- COM1 at 9600 baud
Num
Hold

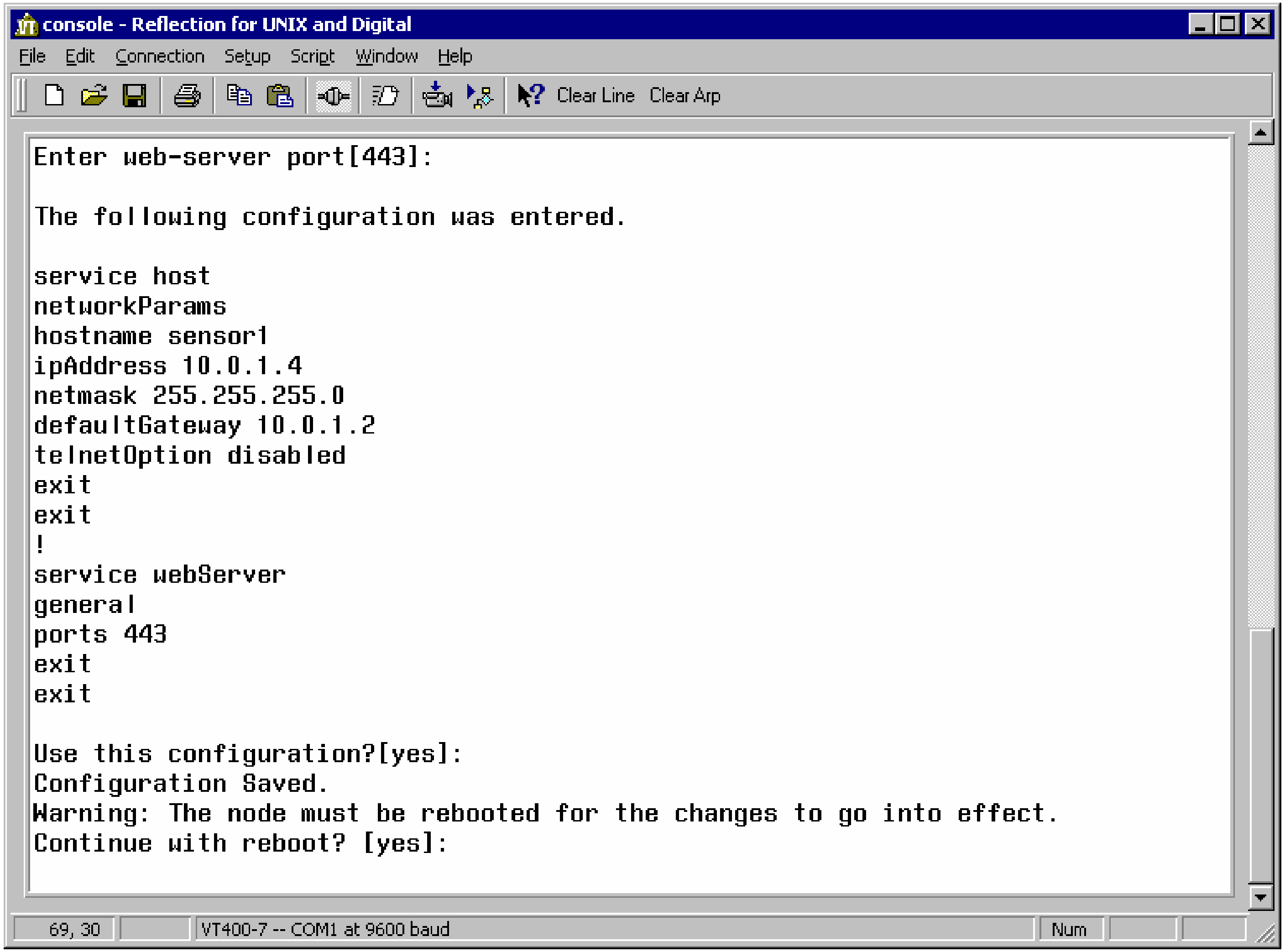
```
sensor# setup


    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
networkParams
hostname sensor
ipAddress 10.1.9.201
netmask 255.255.255.0
defaultGateway 10.1.9.1
telnetOption disabled
exit
exit
!
service webServer
```

Configuration Dialog


console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
Clear Line Clear Arp
66, 31
VT400-7 -- COM1 at 9600 baud
Num
Hold

```
Continue with configuration dialog?[yes]:
Enter host name[sensor]: sensor1
Enter IP address[10.1.9.201]: 10.0.1.4
Enter netmask[255.255.255.0]:
Enter default gateway[10.1.9.1]: 10.0.1.2
Enter telnet-server status[disabled]:
Enter web-server port[443]:

The following configuration was entered.

service host
networkParams
hostname sensor1
ipAddress 10.0.1.4
netmask 255.255.255.0
defaultGateway 10.0.1.2
telnetOption disabled
exit
exit
!
service webServer
general
ports 443
exit
```

Save and Reboot


console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
Clear Line Clear Arp
69, 30
VT400-7 -- COM1 at 9600 baud
Num

```
Enter web-server port[443]:

The following configuration was entered.

service host
networkParams
hostname sensor1
ipAddress 10.0.1.4
netmask 255.255.255.0
defaultGateway 10.0.1.2
telnetOption disabled
exit
exit
!
service webServer
general
ports 443
exit
exit

Use this configuration?[yes]:
Configuration Saved.
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]:
```

Command Line Modes

CLI Overview

The IDS 4.0 CLI is characterized by the following:

- Provides access to the Sensor via Telnet, SSH, and serial interface connections
- Replaces 3.X OS shell access
- Similar to the IOS CLI

CLI Features

The IDS 4.0 CLI includes the following features:

- Help
- Tab completion
- Abbreviation
- Command recall
- User interactive prompts

CLI Usage

The CLI can be used to perform the following tasks:

- Sensor initialization tasks
- Configuration tasks
- Administrative tasks
- Troubleshooting

CLI Modes

The IDS 4.0 CLI has the following modes:

- Privileged exec
- Global configuration
- Interface command-control configuration
- Interface group configuration
- Interface sensing configuration
- Service
- Virtual sensor configuration
- Alarm channel configuration
- Tune micro engines

Privileged Exec Mode

```
sensor#
```

- Privileged exec mode is the first level of the CLI.
- The following tasks are performed in privileged exec mode:
  - Initialize the Sensor
  - Reboot the Sensor
  - Enter configuration mode
  - Terminate current login session
  - Display system settings
  - Ping

Global Configuration Mode

```
sensor# configure terminal
sensor(config)#
```

- Global configuration mode is the second level of the CLI.
- The following tasks are performed in global configuration mode:
  - Set the Sensor's hostname
  - Create user accounts
  - Configure SSH, Telnet, and TLS settings
  - Re-image the application partition
  - Upgrade and downgrade system software and signatures
  - Enter interface configuration modes
  - Enter service configuration mode

Interface Command-Control Configuration Mode

```
sensor# configure terminal
sensor(config)# interface command-control
sensor(config-if)#
```

- Interface command-control configuration mode is a third level of the CLI.
- The following tasks are performed in interface command-control configuration mode:
  - Configure interface IP information
  - Display system settings

Interface Group Configuration Mode

```
sensor# configure terminal
sensor(config)# interface group 0
sensor(config-ifg)#
```

- Interface group configuration mode is a third level of the CLI.
- The following tasks are performed in interface group configuration mode:
  - Add a sensing interface to the interface group
  - Disable the interface group
  - Display system settings

Interface Sensing Configuration Mode

```
sensor# configure terminal
sensor(config)# interface sensing int1
sensor(config-ifs)#
```

- **Interface sensing configuration mode is a third level of the CLI.**
- **The following tasks are performed in interface sensing configuration mode:**
  - **Enable or disable the sensing interface**
  - **Display system settings**

Service Mode

```
sensor# configure terminal
sensor(config)# service ?
alarm-channel-configuration     Enter configuration mode for the alarm
                                channel
Authentication                  Enter configuration mode for user
                                authentication options
Host                            Enter configuration mode for node
                                configuration
Logger                          Enter configuration mode for debug
                                logger
NetworkAccess                   Enter configuration mode for the
                                network access controller
SshKnownHosts                   Enter configuration mode for
                                configuring SSH known hosts
TrustedCertificates             Enter configuration mode for
                                configuring trusted certificates
virtual-sensor-configuration    Enter configuration mode for the virtual
                                sensor
WebServer                       Enter configuration mode for the web
                                server application
```

- **Sensor configuration mode is a generic command mode.**
- **Enables you to enter configuration mode for various services**

Virtual Sensor Configuration Mode

```
sensor# configure terminal
sensor(config)# service virtual-sensor-configuration
  virtualSensor
sensor(config-vsc)#
```

- Virtual Sensor configuration mode is a third level of the CLI.
- The following tasks are performed in virtual Sensor configuration mode:
  - Reset signature settings to the default configuration
  - Display system settings
  - Enter micro-engine tuning mode

Alarm Channel Configuration Mode

```
sensor# configure terminal
sensor(config)# service alarm-channel-configuration
  virtualAlarm
sensor(config-acc)#
```

- Alarm channel configuration mode is a third level of the CLI.
- The following tasks are performed in alarm channel configuration mode:
  - Display system settings
  - Enter configuration mode for the alarm channel

Tune Micro-Engines Mode

```
sensor# configure terminal
sensor(config)# service virtual-sensor-configuration
  virtualSensor
sensor(config-vsc)# tune-micro-engines
sensor(config-vsc-virtualSensor)#
```

- Tune micro-engines configuration mode is a fourth level of the CLI.
- Enables you to tune micro engines

Cisco.com

Initial Configuration Tasks

Completing the Initial Configuration

After completing the setup command's interactive dialog, complete the initial configuration by doing the following:

- Create user accounts.
- Create a service account.
- Set the system clock.
- Create network access lists.
- Generate a X.509 certificate.
- Add hosts to the SSH known hosts list.

Creating User Accounts

sensor(config)#

```
username name [password password] [privilege
privilege]
```

- Creates a user account

```
sensor(config)# username ADMIN password
  adminpass privilege administrator
```

- Creates the user ADMIN with a privilege level of administrator and the password adminpass

Creating the Service Account

sensor(config)#

```
username name [password password] [privilege
privilege]
```

- Creates a service account

```
sensor(config)# username SERVICE password
  servpass privilege service
```

- Creates a service account called SERVICE with the password servpass

Changing Passwords

sensor(config)#

```
password [name [newPassword ] ]
```

- Changes the password on a user account

```
sensor(config)# password
Enter old login password: *********
Enter new login password: ********
Re-enter new login password: *********
sensor(config)#
```

- Modifies the password for the current user

```
sensor(config)# password OPER
Enter new login password: ******
Re-enter new login password: ******
sensor(config)#
```

- Modifies the password for the operator account, OPER

Changing Privileges

sensor(config)#

```
privilege username [administrator | operator |
viewer]
```

- Changes an account’s role

```
sensor(config)# privilege user TESTUSER
  operator
Warning: The privilege change does not apply
  to current CLI sessions. It will be applied
  to subsequent logins.
sensor(config)#
```

- Changes the role for user TESTUSER to operator

Setting the System Clock

sensor#

```
clock set hh:mm month day year
```

- Sets the system clock

```
sensor# clock set  12:32 January 12 2003
```

- Sets the time to 12:32 pm January 12, 2003

Configuring Network Access

sensor(config-Host-net)#

```
accessList ipAddress ip_address netmask netmask
```

- Creates a network access list

```
sensor# config t
sensor(config)# service host
sensor(config-Host)# networkParams
sensor(config-Host-net)# accessList ipAddress 10.0.1.12
```

- Adds a single host to the access list

```
sensor# config t
sensor(config)# service host
sensor(config-Host)# networkParams
sensor(config-Host-net)# accessList ipAddress 10.0.2.0
  netmask 255.255.255.0
```

- Adds an entire network to the access list

Generating an X.509 Certificate

```
sensor#
```

```
tls generate-key
```

- Generates a self-signed X.509 certificate for the server

```
sensor#  tls generate-key
MD5 fingerprint is
   47:B4:C9:36:B1:E7:D2:5E:D1:3E:F6:B7:83:F4:68:60
   SHA1 fingerprint is
   8B:26:BB:EB:04:D4:9F:27:02:0E:25:F7:BE:0E:91:4F:B8:0A:CF:7B
```

Adding Hosts to the SSH Known Hosts List

sensor(config)#

```
ssh host-key ipaddress [ key-modulus-length
public-exponent public-modulus ]
```

- Adds an entry to the known hosts table

```
sensor(config)# ssh host-key 172.30.1.2
```

- Adds the perimeter router's IP address to the Sensor's list of SSH known hosts

Cisco.com

Preventive Maintenance and Troubleshooting

Displaying the Current Configuration and Version

sensor#

```
show version
```

- Displays version information for all installed OS packages, signature packages, and IDS processes running on the system

.

sensor#

```
more current config
```

- Displays the configuration for the entire system

Displaying Events

sensor#

```
show events [{[alert[informational][low][medium]
[high]] | error [warning | error | fatal ] | log
| NAC | status}][hh:mm:ss[ month day [year]]]
```

- Displays the requested event types beginning at the requested start time

```
sensor# show events alert high 10:00 June 1 2003
```

- Displays all high severity events since 10:00 am June 1, 2003.

Displaying Statistics

```
sensor#
show statistics { Authentication | EventServer |
EventStore | Host | Logger | NetworkAccess |
TransactionServer | TransactionSource |
WebServer } [ clear ]
```

- Displays statistics for the specified service

```
sensor# show statistics EventStore
```

- Displays statistics for the Event Store

Displaying Interface Statistics

```
sensor#
show interfaces [clear]
```

- Displays statistics for all system interfaces

```
sensor#
show interfaces command-control
```

- Displays information about the command and control interface

```
sensor#
show interfaces group [number]
```

- Displays information about the logical interface group

```
sensor#
show interfaces sensing name
```

- Displays information about the sensing interfaces

Displaying Tech Support Information

sensor#

```
show tech-support[page][password][destination
destination-url]
```

- Displays the current system status

```
sensor# show tech-support destination
  ftp://csidsuser@10.2.1.2/reports/sensor1Report.html
  password:*******
```

- Places the tech-support output into the file ~csidsuser/reports/sensor1Report.html

Rebooting the Sensor

sensor#

```
reset [powerdown]
```

- Shuts down the applications running on the Sensor and reboots it

```
sensor# reset
Warning: Executing this command
  will stop all applications and
  reboot the node.
Continue with reset?: yes
  Request Succeeded.
```

Backing Up and Restoring Configurations

```
sensor#
copy [/erase] source-url destination-url
```

- Copies configuration files

```
sensor# copy current-config backup-config
```

- Creates a backup configuration

```
sensor# copy /erase backup-config current-config
```

- Overwrites the current configuration with the back-up configuration

Recovering the Application Partition

sensor(config)#

```
recover application-partition
```

- Re-images the application partition with the application image stored on the recovery partition

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all
  applications and re-image the node to version
  4.0(1)S29. All configuration changes except for
  network settings will be reset to default.
Continue with recovery?:yes
Request Succeeded.
```