Getting Started

IBM BladeCenter PN41 Type 3020 Deep Packet Inspection Blade

This document contains the procedures that you must complete before you can use the IBM® BladeCenter® PN41 Type 3020 Deep Packet Inspection (DPI) Blade.

See the documentation that came with your BladeCenter unit and the documentation on the IBM *Documentation* CD for additional information.

Note: This documentation is intended for experienced users with knowledge of network configurations.

Hardware and software requirements

To set up the DPI blade, you must have the following items:

- VMware ESX Server version 3.0 or later
- VMware Virtual Infrastructure Client 2.0 or later
- A VMware ESX compatible server or blade server
- A 1 Gb Ethernet switch module installed in bay 1 of the BladeCenter unit
- A Nortel Networks Layer 2/3 copper (32R1860) or fiber (32R1861) Ethernet switch module installed in bay 2 of the BladeCenter unit with firmware 1.4.2.0 or later
- 10 Gb switch modules (the number of switches depends on applications)
- A RAVE application, or the ability to create a RAVE application, using an Integrated Development Environment
- An IBM advanced management module installed in the BladeCenter unit
- CloudShield PacketWorks Operating System (CPOS) software download
- A remote console with Microsoft® Internet Explorer 6.0 or later

Two network interface connection ports are used in the configuration of the DPI blade. One port is used for management access, such as through the CloudShield Web Management Interface or a command-line interface (CLI) over Secure Shell (SSH). The other port is used to communicate with the Deep Packet Processing Module (DPPM). The DPI management and CPOS management must be on different subnets.

Performance of the DPI blade varies, depending on the following factors:

- The application that is being deployed
- The packet size
- The DPI blade configuration
- The type of traffic

Configuration summary

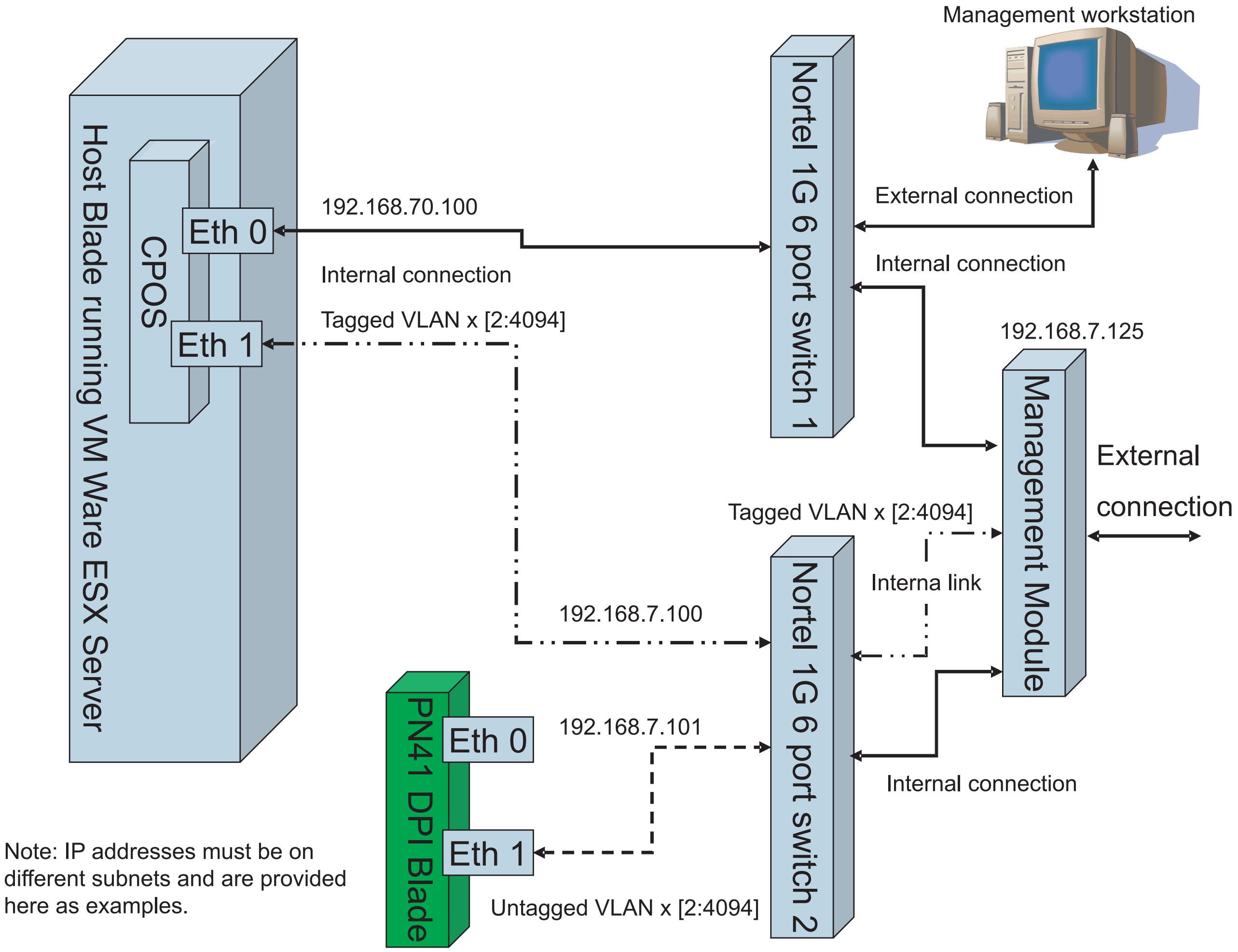
The following overview summarizes the tasks that you must complete to make the DPI blade operational. The order of the tasks in this overview differs from the order of the actual steps. For step-by-step instructions, see "Setting up and configuring the DPI blade" on page 4.

- Configure the management module:
  - Enable SNMPv1 and add the CPOS control port IP address to the public community, or set SNMPv1 to the defaults.
  - Set the TCP command mode protocol to *n* + *m*, where *n* is the number of DPI blades in the BladeCenter unit and *m* is the number of TCP command mode protocol connections that currently exist.
- Configure the chassis internal network (CIN):
  - Set the IP addresses of the CPOS management port.
  - Create a management VLAN and add ports on a CIN-supported switch module.
  - Enable the chassis internal network (CIN) and set the IP addresses in the advanced management module.
- Install and configure the VMware ESX Server virtual machine:
  - Create a virtual switch for the DPPM network.
  - Select Red Hat Enterprise Linux 4 as the operating-system type.
  - Select one processor with 1024 MB of memory. Select two NICs (one for the VM network and one for the DPPM network). Create an LSI Logic virtual disk with a minimum size of 10 Gb.
  - Configure the virtual machine BIOS boot order to be **Hard Drive** and then **CD-ROM Drive**.
  - Install the CPOS on the virtual machine.
- Configure the CloudShield PacketWorks Operating System:
  - The default user ID is `admin`, and the default password is `cloudshield`.
  - Set the IP address of the management port (eth0).

    Note: The CPOS management port must be on a different subnet than the BladeCenter advanced management module.
  - Set the IP address of the control port (eth1).

    Note: The CPOS control port must be on the same subnet as the BladeCenter advanced management module.
  - See "Setting up and configuring the DPI blade" on page 4 for command-line configuration options to configure the Application Server Module (ASM) network.

The following illustration shows an example configuration that uses the DPI blade. The 192.168.7.*xxx* subnetwork uses VLAN ID 4094 to communicate internally within the BladeCenter unit and is used as the CPOS control network. The 192.168.70.*xxx* subnetwork is used as the CPOS management network. The IP addresses and the VLAN ID are shown for illustrative purposes only.



DPI blade IP addresses

Use this table to record the IP addresses that you set during configuration. You will need these IP addresses when you set up the DPI blade.

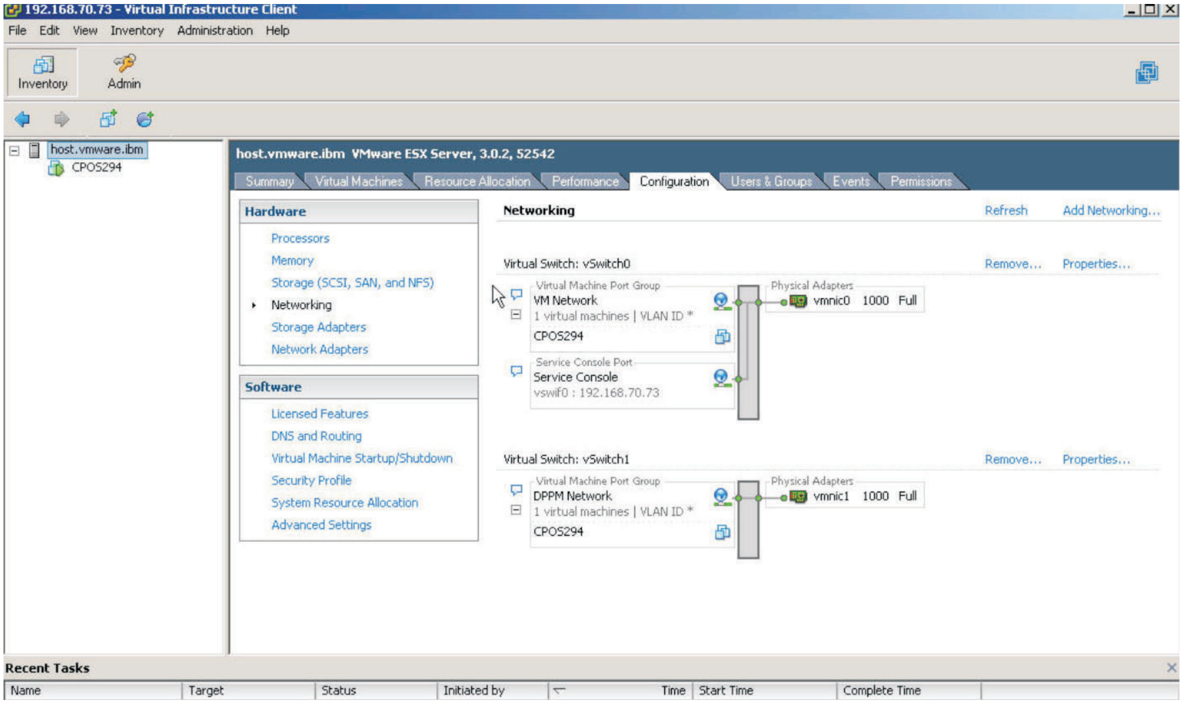
Table 1. IP addresses

ID	IP address	Notes
BladeCenter advanced management module IP address		
CPOS eth0		Internal connection to switch bay 1
CPOS eth1		Tagged VLAN to switch bay 2
DPI blade eth1		Untagged VLAN to switch bay 2
VLAN ID		
Host blade server		

Setting up and configuring the DPI blade

To set up and configure the DPI blade, complete the following steps:

1. Enable the SNMPv1 agent:
   a. From the remote console, log in to the advanced management module in the BladeCenter unit and start a session.
   b. Select **MM Control → Network Protocol**. Under **Management Module Network Protocols**, select **Simple Network Management Protocol** (SNMP).
   c. From the menu, select **Enabled** for the SNMPv1 agent. Click **Save**.
   d. Under **Management Module Network Protocols**, select **TCP Command Mode Protocol**. Set the **Command Mode** field to *n* + *m*, where *n* is the number of DPI blades in the BladeCenter unit and *m* is the number of TCP command mode protocol connections that currently exist.
2. Install VMware ESX Server on the host (client) blade server. Follow the installation instructions that come with the software. During the installation, specify a user name and password, and assign an IP address to the host blade server. Record this IP address in "DPI blade IP addresses" on page 3.
3. Install VMware Virtual Infrastructure Client 2.0 on the remote console. Follow the installation instructions that come with the software.
4. Add a virtual switch:
   a. From Virtual Infrastructure Client on the remote console, log in to the host blade server, using the IP address, user name, and password that you specified in step 2.
   b. Click the **Configuration** tab.
   c. Under **Hardware**, click **Networking**, and click **Add Networking**.



192.168.70.73 - Virtual Infrastructure Client

host.vmware.ibm VMware ESX Server, 3.0.2, 52542

Networking

Virtual Switch: vSwitch0

Virtual Machine Port Group: VM Network, 1 virtual machines | VLAN ID *, CPOS294

Service Console Port: Service Console, vswif0 : 192.168.70.73

Physical Adapters: vmnic0 1000 Full

Virtual Switch: vSwitch1

Virtual Machine Port Group: DPPM Network, 1 virtual machines | VLAN ID *, CPOS294

Physical Adapters: vmnic1 1000 Full

   d. Select **Virtual Machine**, and click **Next**.
   e. Select **Create a Virtual Switch**, and click **Next**.
   f. In the **VLAN ID** field, enter an unused VLAN ID number between 2 and 4094. Record the VLAN ID in "DPI blade IP addresses" on page 3.

Note: This is the VLAN ID of the chassis internal network, where the host blade server communicates with the advanced management module.

g. In the **Network Label** field, type `DPPM Network`. Click **Next**, and click **Finish**.

5. Create a virtual machine in the host blade server:

   a. Click **File** → **New** → **Virtual Machine**.

   b. Select **Custom**, and click **Next**.

   c. In the **Virtual Machine Name** field, type a name for the virtual machine. Click **Next**.

   d. Select the datastore in which to store files for the virtual machine.

   e. Select **Linux**®; then, select **Red Hat Enterprise Linux 4** from the menu. Click **Next**.

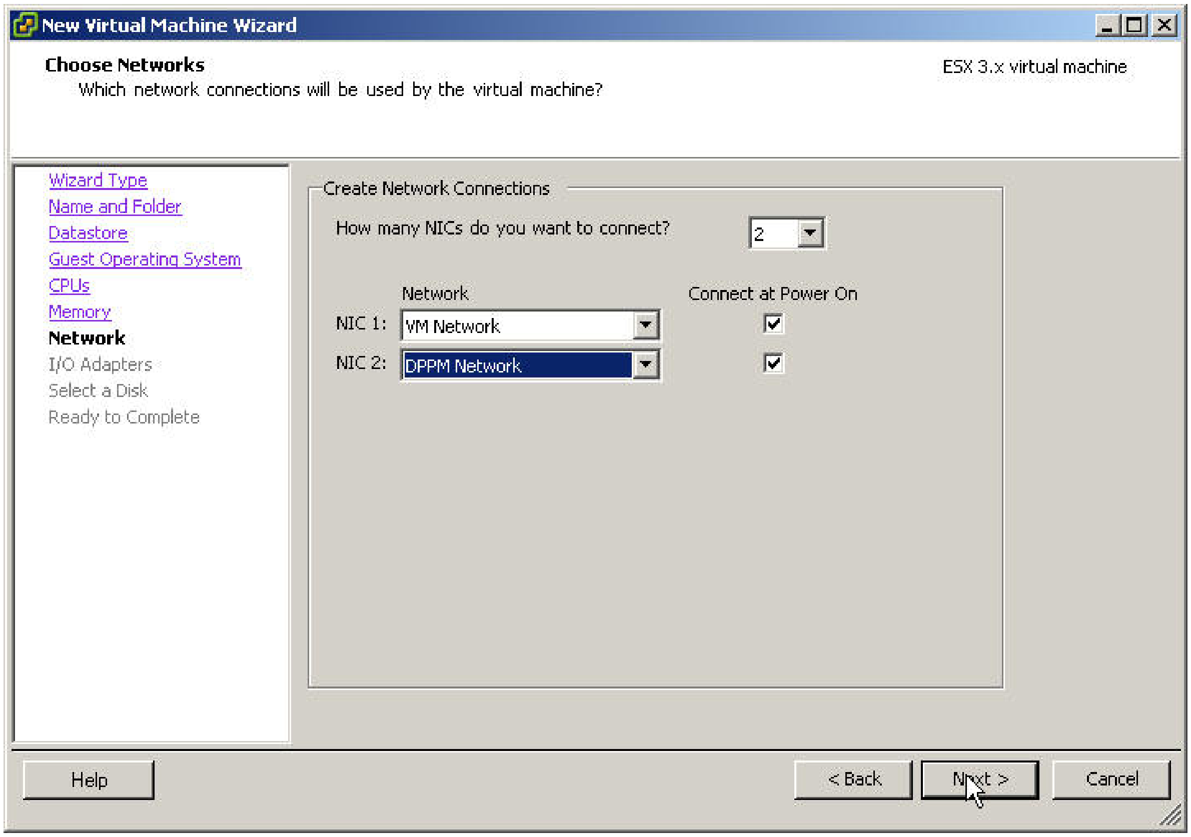
   Attention: You must select the correct version of Linux for compatibility with the CloudShield PacketWorks Operating System (CPOS).

   f. In the **Number of virtual processors** field, select **1**. Click **Next**.

   g. In the **Memory for the virtual machine** field, select **1024 MB**. Click **Next**.

   h. In the **How many NICs do you want to connect** field, select **2**. In the **NIC 1** field, select **VM Network**. In the **NIC 2** field, select **DPPM Network**.

   i. Select the **Connect at Power On** check box for each NIC. Click **Next**.



New Virtual Machine Wizard

Choose Networks

Which network connections will be used by the virtual machine?

ESX 3.x virtual machine

Create Network Connections

How many NICs do you want to connect? 2

	Network	Connect at Power On
NIC 1:	VM Network	☑
NIC 2:	DPPM Network	☑

   j. Select **LSI Logic**. Click **Next**.

   k. Select **Create a new virtual disk**. Click **Next**.

   l. Under **Disk Capacity** → **Disk Size**, select at least 10 Gb; then, select **Store with the virtual machine**. Click **Next**.

   m. Click **Next**, and click **Finish**.

6. Configure the virtual machine BIOS.

Note: Each virtual machine has its own independent BIOS setting. An alternative method is to place the ISO image on the host blade server and mount the virtual CD drive with the ISO image. If you mount the ISO image on the client, the host blade server might not automatically eject the virtual CD as required at the end of the installation, and you might have to eject the CD manually. The installation will start over if you do not eject the CD.

a. From the left pane, select the virtual machine that you created in step 5.

b. Click the **Console** tab.

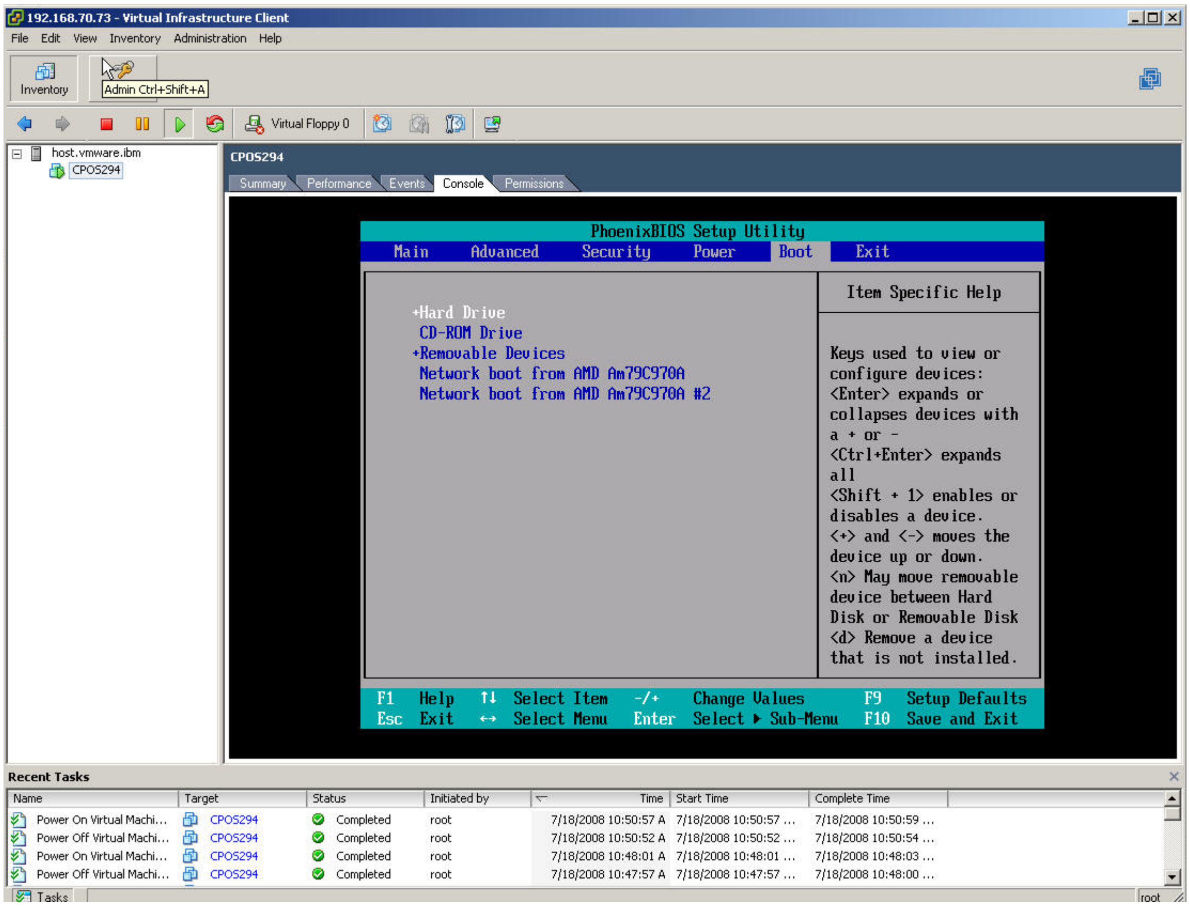
Important:: In the following step, you must press F2 while the VMware screen is displayed. If you fail to do this, press Ctrl+Alt to release the cursor from the console window, and click the **Reset** icon to restart the boot process.

c. Click the **Power on** icon and click inside the console window. When the VMware screen is displayed, press F2.

d. Using the Right Arrow key, highlight **Boot**.

e. Using the Down Arrow key, highlight **Hard Drive**; then, press + to move **Hard Drive** to the top of the list.

f. Using the Down Arrow key, highlight **CD-ROM Drive**; then, press + to move **CD-ROM Drive** to the second position in the list.



```
                    PhoenixBIOS Setup Utility
  Main     Advanced     Security     Power     Boot     Exit

                                                Item Specific Help
      +Hard Drive
       CD-ROM Drive                           Keys used to view or
      +Removable Devices                      configure devices:
       Network boot from AMD Am79C970A        <Enter> expands or
       Network boot from AMD Am79C970A #2     collapses devices with
                                              a + or -
                                              <Ctrl+Enter> expands
                                              all
                                              <Shift + 1> enables or
                                              disables a device.
                                              <+> and <-> moves the
                                              device up or down.
                                              <n> May move removable
                                              device between Hard
                                              Disk or Removable Disk
                                              <d> Remove a device
                                              that is not installed.

  F1   Help  ↑↓  Select Item  -/+    Change Values        F9   Setup Defaults
  Esc  Exit  ↔   Select Menu  Enter  Select ▶ Sub-Menu    F10  Save and Exit
```

Recent Tasks

Name	Target	Status	Initiated by	Time	Start Time	Complete Time
Power On Virtual Machi...	CPOS294	Completed	root	7/18/2008 10:50:57 A	7/18/2008 10:50:57 ...	7/18/2008 10:50:59 ...
Power Off Virtual Machi...	CPOS294	Completed	root	7/18/2008 10:50:52 A	7/18/2008 10:50:52 ...	7/18/2008 10:50:54 ...
Power On Virtual Machi...	CPOS294	Completed	root	7/18/2008 10:48:01 A	7/18/2008 10:48:01 ...	7/18/2008 10:48:03 ...
Power Off Virtual Machi...	CPOS294	Completed	root	7/18/2008 10:47:57 A	7/18/2008 10:47:57 ...	7/18/2008 10:48:00 ...

g. Press F10. Select **Yes**, and press Enter.

7. Install the CloudShield PacketWorks Operating Sytem (CPOS) on the virtual machine:

   a. See *CPOS download for the IBM PN41 DPI blade* on the IBM *Documentation* CD. For more information about installing an image under VMware, or for alternative methods, see http://www.vmware.com/.

   b. Click the **Summary** tab. Under **Commands**, select **Edit Settings**.

   c. Select **CD/DVD Drive 1**. Under **Device Type**, select **client device**.

   d. Select the **Connect at power on** check box, and click **OK**.

e. Click the **Console** tab. Power-on the virtual machine by clicking the **Power On** icon, or reset the virtual machine by clicking the **Reset** icon.

f. When the CloudShield Recovery CD screen is displayed at the beginning of the installation, select the operating-system security standard (rescue-permissive or rescue-enforcing) and press Enter.

Notes:

1) If you press Enter without selecting a security standard, rescue-enforcing is used as the default.

2) Contact your system administrator for more information about permissive and enforcing modes.

3) Package installation screens are displayed during the installation.

g. After the installation, eject the CD or disconnect the ISO image from the virtual CD drive.

h. When the POST installation screen is displayed, select the first option that is shown or wait for the timeout, which defaults to the first selection. The system restarts.

i. Type the default user name, `admin`, and the default password, `cloudshield`. You can change the user name and password after the setup is complete. For more information, see the CloudShield *Web Management Interface Users Guide* on the IBM *Documentation* CD.

Note: When you type the password, the cursor does not move, and the password is not displayed.

j. At the command prompt, type the following commands. After each command, press Enter.

```
admin@CloudShield!> set asm port=eth0 ipaddress=ipaddress netmask=netmask admin=enable
role=management

admin@CloudShield!> set asm port=eth1 ipaddress=ipaddress netmask=netmask admin=enable
role=control

admin@CloudShield!> set route 0.0.0.0 netmask=0.0.0.0 gateway=gateway

admin@CloudShield!> set service http adminstate=enabled

admin@CloudShield!> set authhost 0.0.0.0 netmask=0.0.0.0 ruleOrder=1 httpsAccess=enabled
httpAccess=enabled
```

ipaddress, *netmask*, and *gateway* are the IP address, netmask, and gateway that are to be assigned to the virtual machine. Record these IP addresses in “DPI blade IP addresses” on page 3.

Notes:

1) The IP address of eth0 (the CPOS management port) must be on a different subnetwork than the advanced management module.

2) The IP address of eth1 (the CPOS control port) must be on the same subnetwork as the advanced management module.

3) The gateway must be on the same subnet as eth0.

You now have access to the CloudShield Web Management Interface and the services that you enabled. For information about the command-line interface (CLI) command syntax and options, see the *Command Line Interface Reference Guide* on the IBM *Documentation* CD.

8. Configure the chassis internal network:

a. Log in to the advanced management module.

b. Under **MM Control** in the left pane, select **Chassis Internal Network** .

c. From the **Chassis Internal Network Configuration** menu, select **Enabled**.

d. Select an unused **CIN VLAN ID** link to define the first CIN entry.

e. On the Chassis Internal Network Entry Definition page, enter the VLAN ID that you specified in step 4f. In the **CTRL** field, enter the IP address of eth1. Click **Save**. Record the IP address in “DPI blade IP addresses” on page 3.

f. Under **I/O Module Tasks** in the left pane, select **Configuration**.

g. Click **Bay 2** and select **Advanced Configuration**.

h. Scroll down and click **Start Web Session** to display the switch module administration page.

i. Enter the switch module login information, and click **OK**.

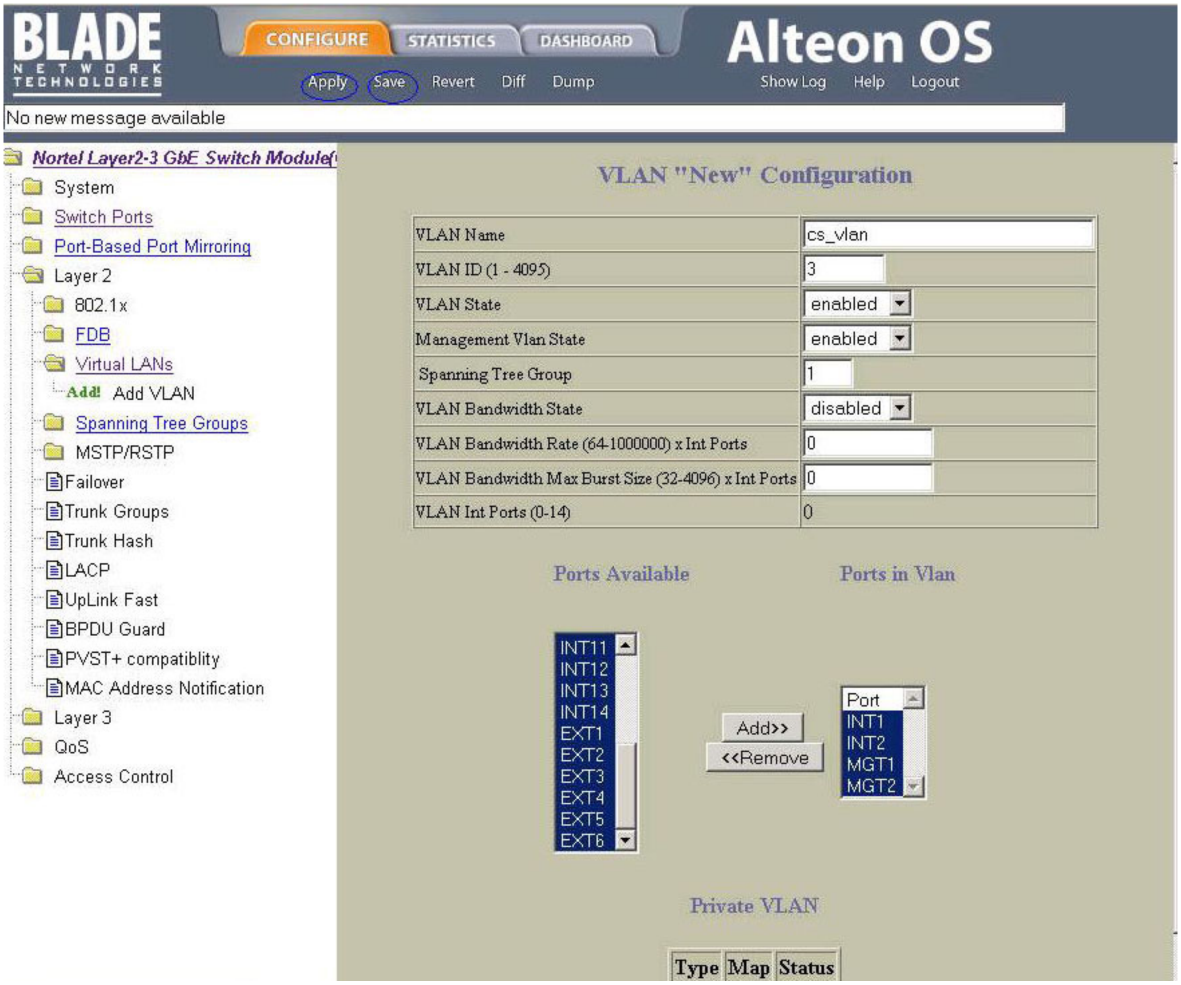
j. Click the **Configure** tab. In the left pane, select the Nortel Layer 2-3 GbE Switch Module folder, select the Layer 2 folder, and select the Virtual LANs folder. Click **Add!**.

k. In the **VLAN Name** field, enter the VLAN ID that you specified in step 4f.

l. From the **VLAN State** menu, select **enabled**. From the **Management VLAN State** menu, select **enabled**.

m. Add the ports that are associated with the host blade server and the DPI blade to the **Ports in Vlan** list.

n. Add the MGT1 and MGT2 ports to the **Ports in Vlan** list.



No new message available

VLAN "New" Configuration

VLAN Name	cs_vlan
VLAN ID (1 - 4095)	3
VLAN State	enabled
Management Vlan State	enabled
Spanning Tree Group	1
VLAN Bandwidth State	disabled
VLAN Bandwidth Rate (64-1000000) x Int Ports	0
VLAN Bandwidth Max Burst Size (32-4096) x Int Ports	0
VLAN Int Ports (0-14)	0

Ports Available	Ports in Vlan
INT11 INT12 INT13 INT14 EXT1 EXT2 EXT3 EXT4 EXT5 EXT6	Port INT1 INT2 MGT1 MGT2

Private VLAN

Type	Map	Status

o. Click **Submit**. Click **Apply**. Click **Save**.

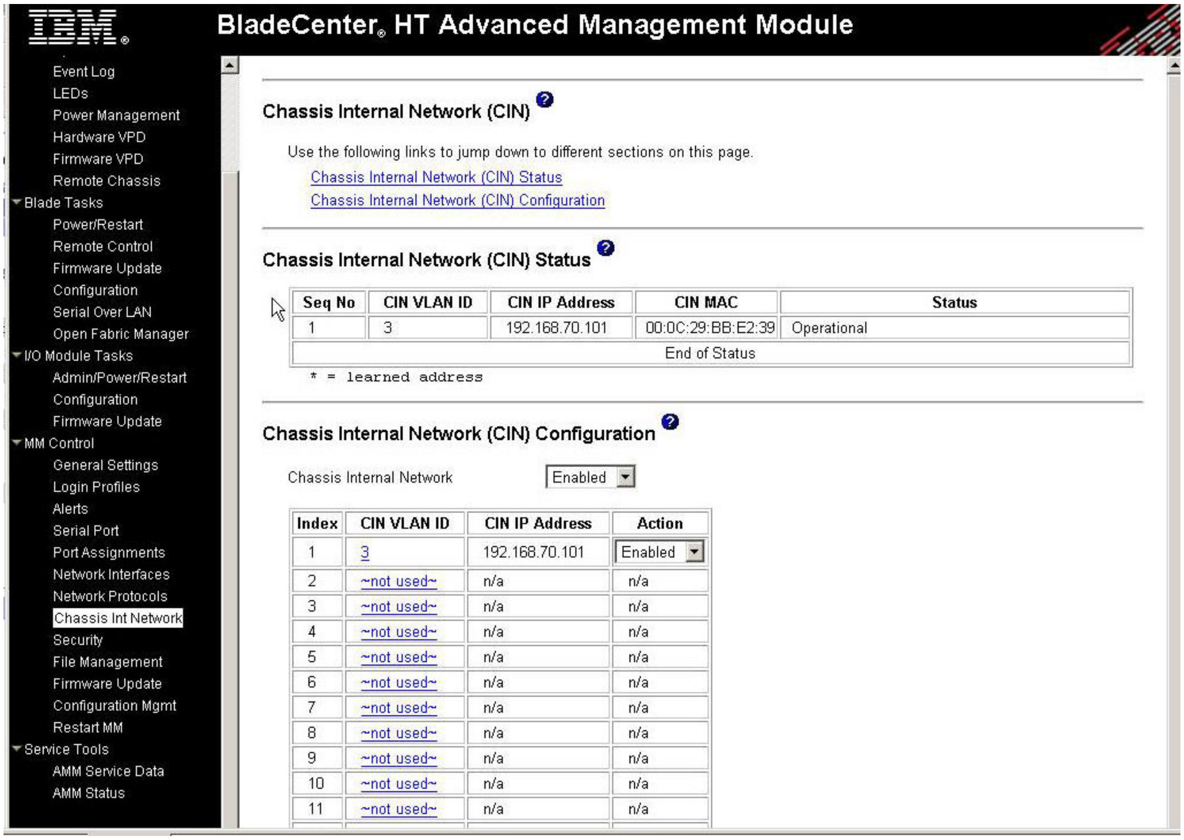
Note: In the list of VLAN ports, INT1 through INT14 are associated with blade bays 1 through 14 in BladeCenter H units, and INT13 and INT14 are associated with the interswitch links (ISL) in BladeCenter HT units.

p. In the left pane, click **Switch Ports**. Select the switch port that is associated with the DPI blade.

q. For each DPI blade, set the **Default Port VLAN ID** to the VLAN ID that you specified in step 4f.

r. Click **Submit**. Click **Apply**. Click **Save**.

s. Log in to the advanced management module and select **Chassis Internal Network** from the left pane. Make sure that the status is Operational and a CIN MAC address is shown.



Chassis Internal Network (CIN)

Use the following links to jump down to different sections on this page.

Chassis Internal Network (CIN) Status
Chassis Internal Network (CIN) Configuration

Chassis Internal Network (CIN) Status

Seq No	CIN VLAN ID	CIN IP Address	CIN MAC	Status
1	3	192.168.70.101	00:0C:29:BB:E2:39	Operational
End of Status				

* = learned address

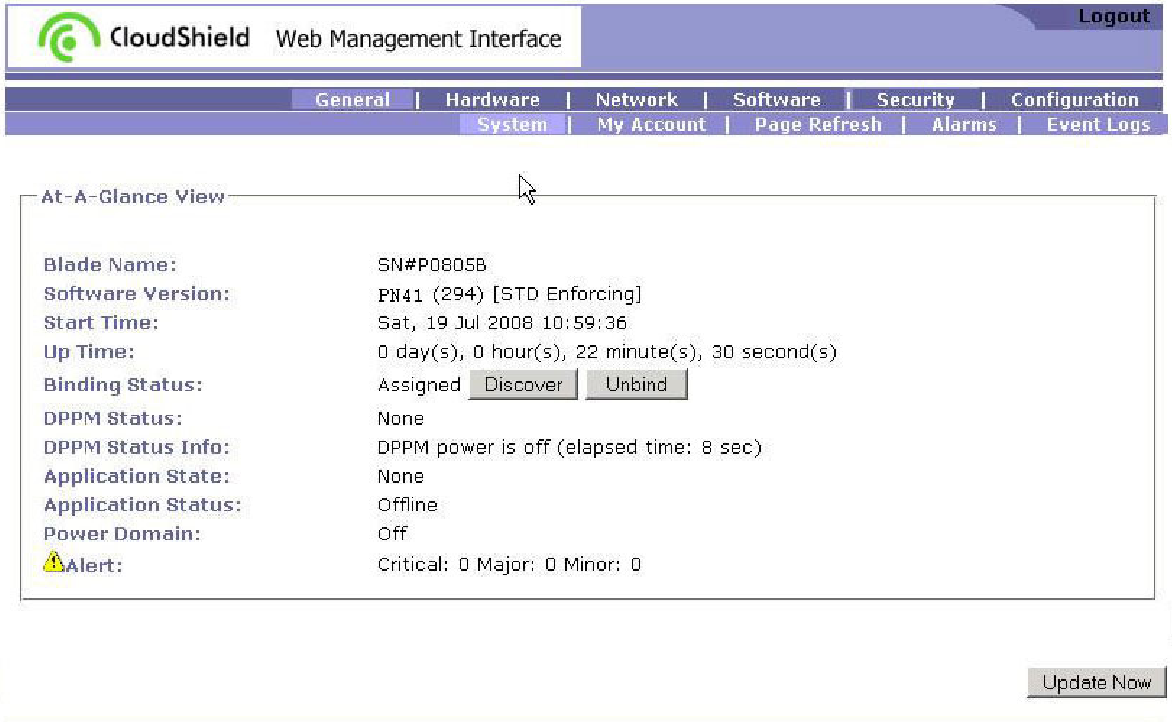
Chassis Internal Network (CIN) Configuration

Chassis Internal Network: Enabled

Index	CIN VLAN ID	CIN IP Address	Action
1	3	192.168.70.101	Enabled
2	~not used~	n/a	n/a
3	~not used~	n/a	n/a
4	~not used~	n/a	n/a
5	~not used~	n/a	n/a
6	~not used~	n/a	n/a
7	~not used~	n/a	n/a
8	~not used~	n/a	n/a
9	~not used~	n/a	n/a
10	~not used~	n/a	n/a
11	~not used~	n/a	n/a

9. Configure the CloudShield PacketWorks Operating System (CPOS):
   a. Log in to the CloudShield Web Management Interface.
   b. From a system on the same network as the virtual machine, open Microsoft Internet Explorer. In the address bar, type the IP address that you assigned to the virtual machine in step 7j.
   c. In the **Login Name** and **Password** fields, type the user name and password.

      Note: The default user name is `admin`, and the default password is `cloudshield`. You can change the user name and password when setup is complete.
   d. Select **Terminate existing session and login as you are**. Click **Apply**.
   e. Click the **General** tab. Make sure that the binding status is Available, and then click **Bind**.

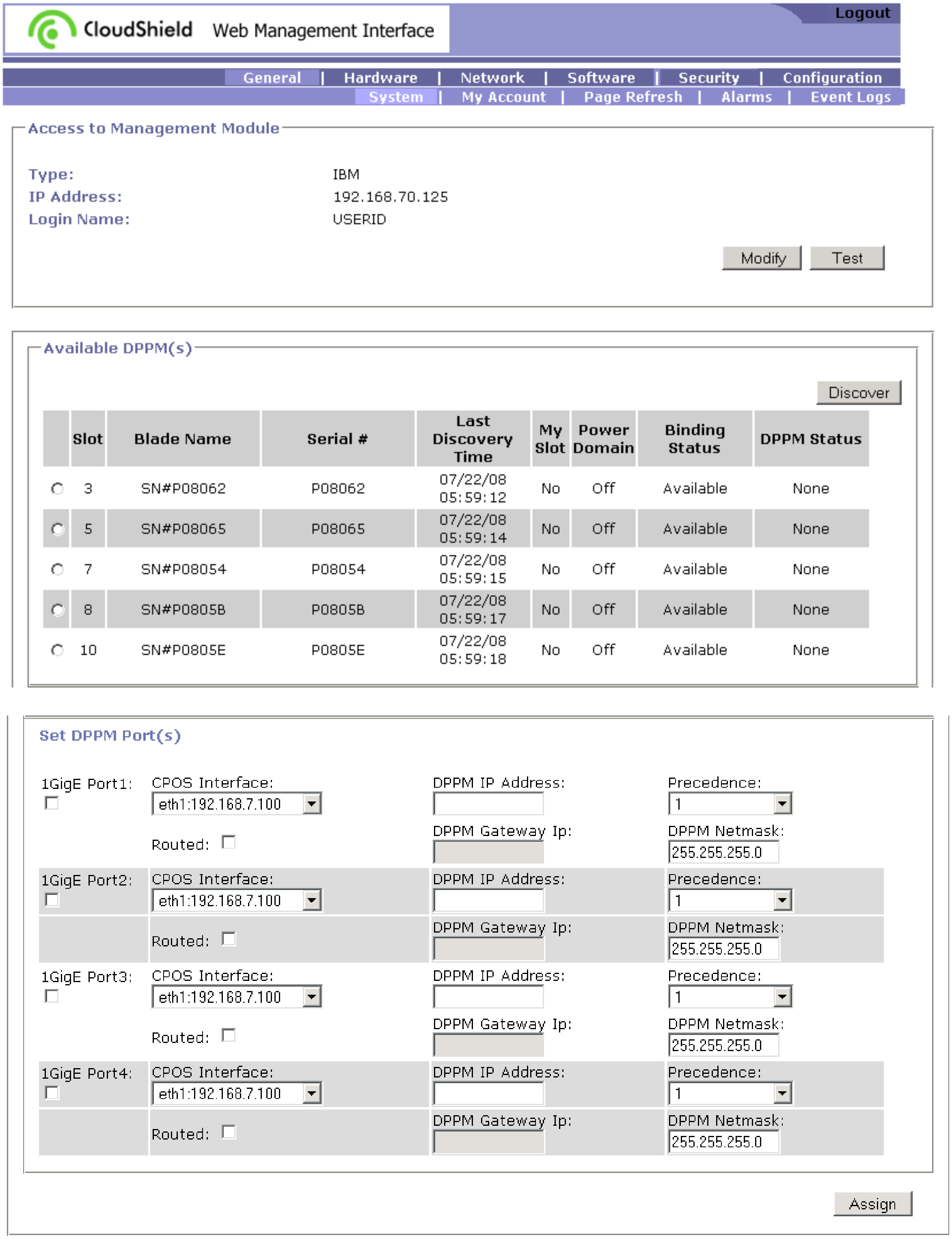

CloudShield Web Management Interface
Logout
General | Hardware | Network | Software | Security | Configuration
System | My Account | Page Refresh | Alarms | Event Logs
Discover
Unbind
Update Now

At-A-Glance View

Blade Name:	SN#P0805B
Software Version:	PN41 (294) [STD Enforcing]
Start Time:	Sat, 19 Jul 2008 10:59:36
Up Time:	0 day(s), 0 hour(s), 22 minute(s), 30 second(s)
Binding Status:	Assigned
DPPM Status:	None
DPPM Status Info:	DPPM power is off (elapsed time: 8 sec)
Application State:	None
Application Status:	Offline
Power Domain:	Off
⚠Alert:	Critical: 0 Major: 0 Minor: 0

   f. Click **Modify**.
   g. In the **IP Address** field, type the IP address of the advanced management module and enter the login name and password for the advanced management module. Click **Apply**.
   h. Click **Test**. If there is communication with the advanced management module, `OK` is displayed.
   i. Click **Discover** and select the slot of the DPI blade that you want to bind to the Application Server Module (ASM).
   j. From the **Available DPPM(s)** list, select your DPI blade.

k. Select the **1GigE Port2** check box. From the **CPOS Interface** menu, select the ASM eth1 IP address. In the **DPPM IP Address** field, type an IP address of the DPPM, on the same subnetwork as the CPOS interface Ethernet device. Click **Assign**.


CloudShield Web Management Interface
Logout
General | Hardware | Network | Software | Security | Configuration
System | My Account | Page Refresh | Alarms | Event Logs
Modify
Test
Discover
Assign

Access to Management Module

Type:	IBM
IP Address:	192.168.70.125
Login Name:	USERID

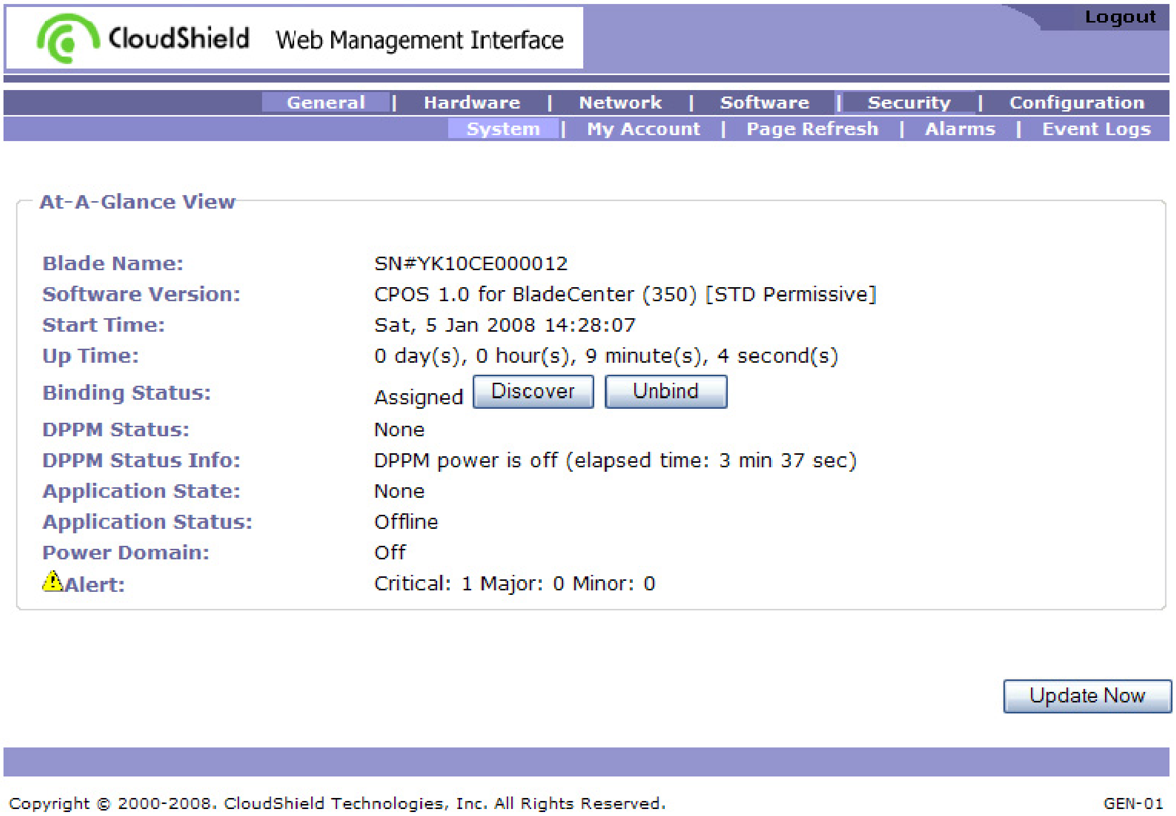
Available DPPM(s)

	Slot	Blade Name	Serial #	Last Discovery Time	My Slot	Power Domain	Binding Status	DPPM Status
○	3	SN#P08062	P08062	07/22/08 05:59:12	No	Off	Available	None
○	5	SN#P08065	P08065	07/22/08 05:59:14	No	Off	Available	None
○	7	SN#P08054	P08054	07/22/08 05:59:15	No	Off	Available	None
○	8	SN#P0805B	P0805B	07/22/08 05:59:17	No	Off	Available	None
○	10	SN#P0805E	P0805E	07/22/08 05:59:18	No	Off	Available	None

Set DPPM Port(s)

1GigE Port1: □	CPOS Interface: eth1:192.168.7.100	DPPM IP Address:	Precedence: 1
	Routed: □	DPPM Gateway Ip:	DPPM Netmask: 255.255.255.0
1GigE Port2: □	CPOS Interface: eth1:192.168.7.100	DPPM IP Address:	Precedence: 1
	Routed: □	DPPM Gateway Ip:	DPPM Netmask: 255.255.255.0
1GigE Port3: □	CPOS Interface: eth1:192.168.7.100	DPPM IP Address:	Precedence: 1
	Routed: □	DPPM Gateway Ip:	DPPM Netmask: 255.255.255.0
1GigE Port4: □	CPOS Interface: eth1:192.168.7.100	DPPM IP Address:	Precedence: 1
	Routed: □	DPPM Gateway Ip:	DPPM Netmask: 255.255.255.0

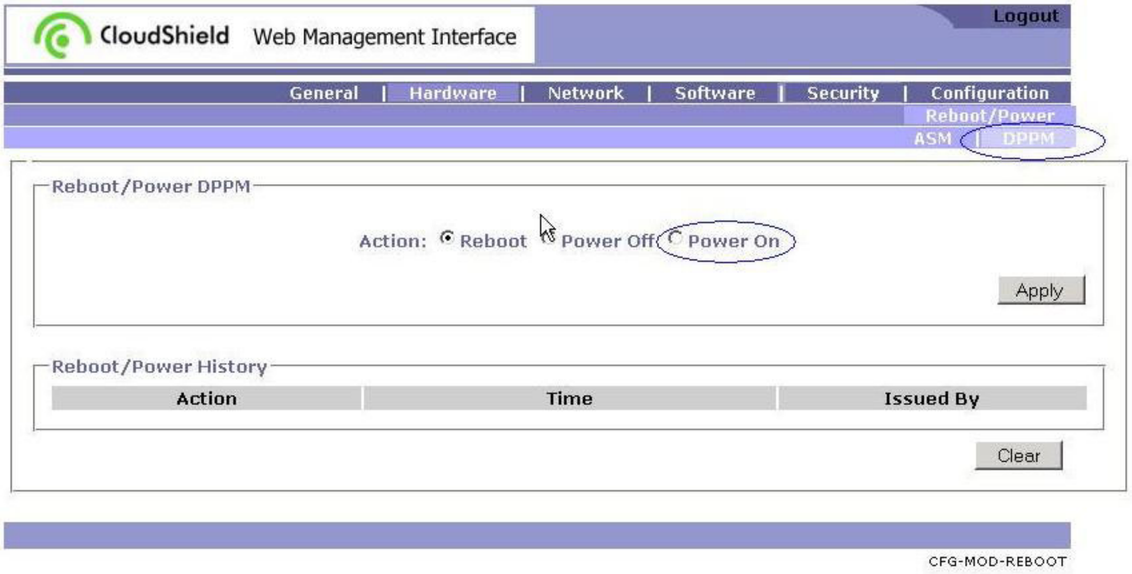
Note: Make sure that the binding status is Assigned.


CloudShield Web Management Interface
Logout
General | Hardware | Network | Software | Security | Configuration
System | My Account | Page Refresh | Alarms | Event Logs
Discover
Unbind
Update Now
GEN-01

At-A-Glance View

Blade Name:	SN#YK10CE000012
Software Version:	CPOS 1.0 for BladeCenter (350) [STD Permissive]
Start Time:	Sat, 5 Jan 2008 14:28:07
Up Time:	0 day(s), 0 hour(s), 9 minute(s), 4 second(s)
Binding Status:	Assigned
DPPM Status:	None
DPPM Status Info:	DPPM power is off (elapsed time: 3 min 37 sec)
Application State:	None
Application Status:	Offline
Power Domain:	Off
⚠Alert:	Critical: 1 Major: 0 Minor: 0

l. Turn on the DPPM modules:
   1) Click the **Hardware** tab.
   2) Click **DPPM**.
   3) Select **Power On**, and click **Apply**.


CloudShield Web Management Interface
Logout
General | Hardware | Network | Software | Security | Configuration
Reboot/Power
ASM | DPPM
Apply
Clear
CFG-MOD-REBOOT

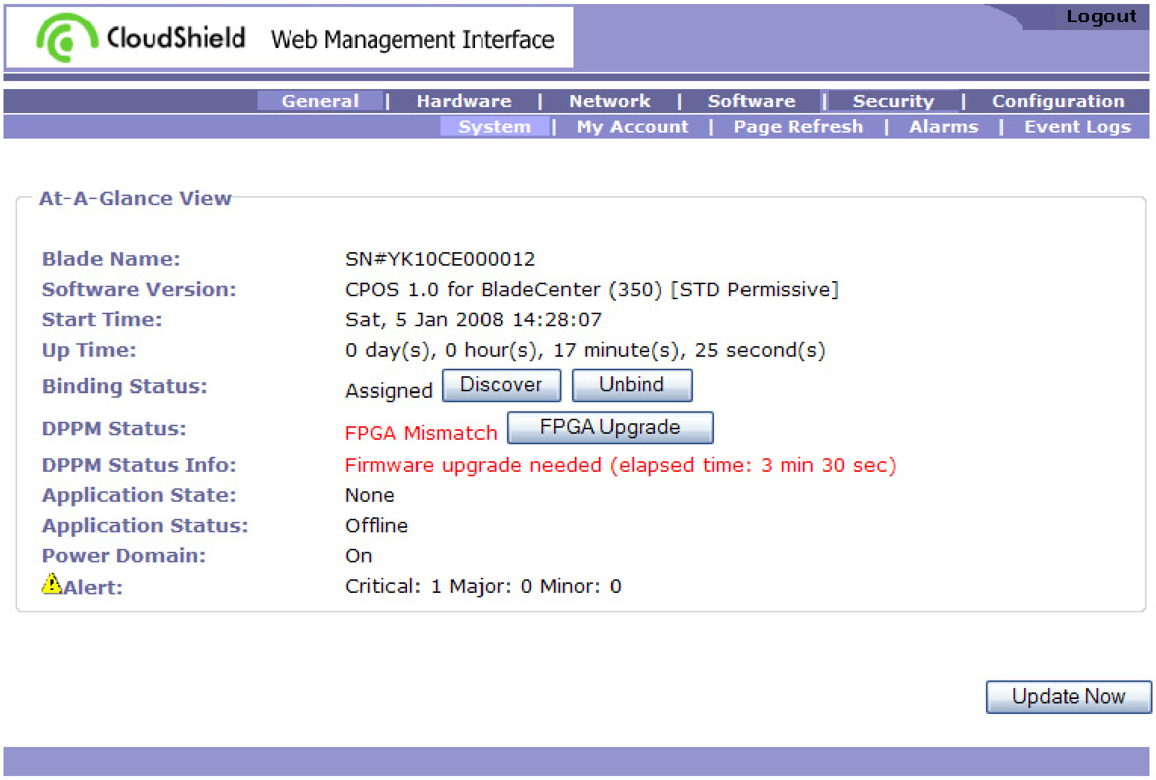
Reboot/Power DPPM

Action: ● Reboot ○ Power Off ○ Power On

Reboot/Power History

Action	Time	Issued By

m. Click the **General** tab. Click **Update Now**. If the DPI blade is current, the DPPM status is Bonded. If the blade must be updated, the DPPM status is FPGA Mismatch. To update the FPGA (field programmable gate array), click **FPGA Upgrade** and click **OK**.


CloudShield Web Management Interface
Logout
General | Hardware | Network | Software | Security | Configuration
System | My Account | Page Refresh | Alarms | Event Logs
Discover
Unbind
FPGA Upgrade
Update Now

At-A-Glance View

Blade Name:	SN#YK10CE000012
Software Version:	CPOS 1.0 for BladeCenter (350) [STD Permissive]
Start Time:	Sat, 5 Jan 2008 14:28:07
Up Time:	0 day(s), 0 hour(s), 17 minute(s), 25 second(s)
Binding Status:	Assigned
DPPM Status:	FPGA Mismatch
DPPM Status Info:	Firmware upgrade needed (elapsed time: 3 min 30 sec)
Application State:	None
Application Status:	Offline
Power Domain:	On
⚠Alert:	Critical: 1 Major: 0 Minor: 0

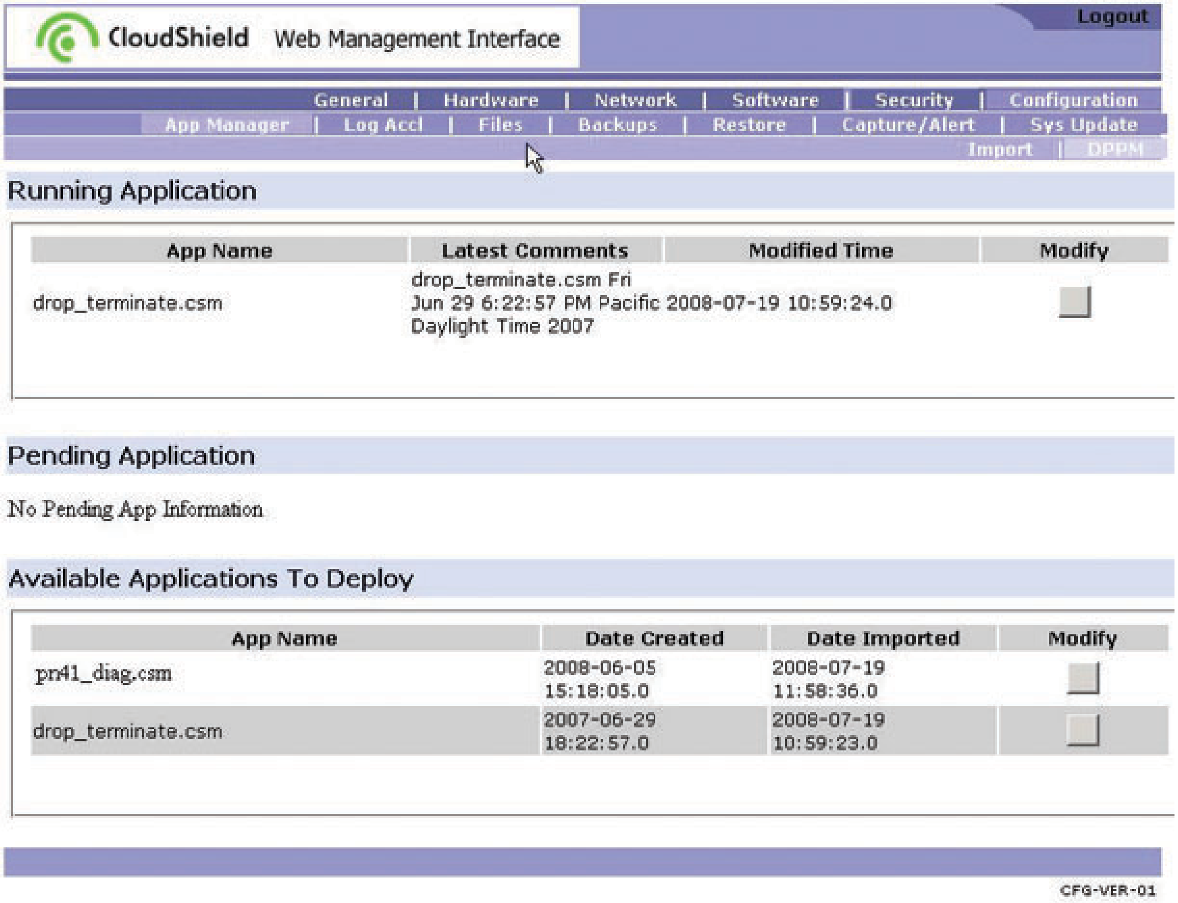
Note: Do not power-off or remove the blade during the FPGA upgrade process. Applications will not be installed until the FPGA upgrade is complete. To see the current status of the upgrade process, click **Update Now**. The upgrade process can take up to 10 minutes. After the FPGA upgrade is complete, the DPPM status is Bonded.

10. Install applications on the DPI blade:
   a. Click the **Configuration** tab.
   b. In the **Upload Application File** area, click **Browse**, select a file from the **App File** list, and click **Upload**.

c. From **Import Application File** list, select the application file that is to be imported, and click **Import**.

d. Click **Yes** to import the file.

e. Click **DPPM**. Select the available application to install by selecting the **Modify** check box beside the application name.


CloudShield Web Management Interface
Logout
General | Hardware | Network | Software | Security | Configuration
App Manager | Log Accl | Files | Backups | Restore | Capture/Alert | Sys Update
Import | DPPM

Running Application

App Name	Latest Comments	Modified Time	Modify
drop_terminate.csm	drop_terminate.csm Fri Jun 29 6:22:57 PM Pacific Daylight Time 2007	2008-07-19 10:59:24.0	☐

Pending Application

No Pending App Information

Available Applications To Deploy

App Name	Date Created	Date Imported	Modify
pn41_diag.csm	2008-06-05 15:18:05.0	2008-07-19 11:58:36.0	☐
drop_terminate.csm	2007-06-29 18:22:57.0	2008-07-19 10:59:23.0	☐

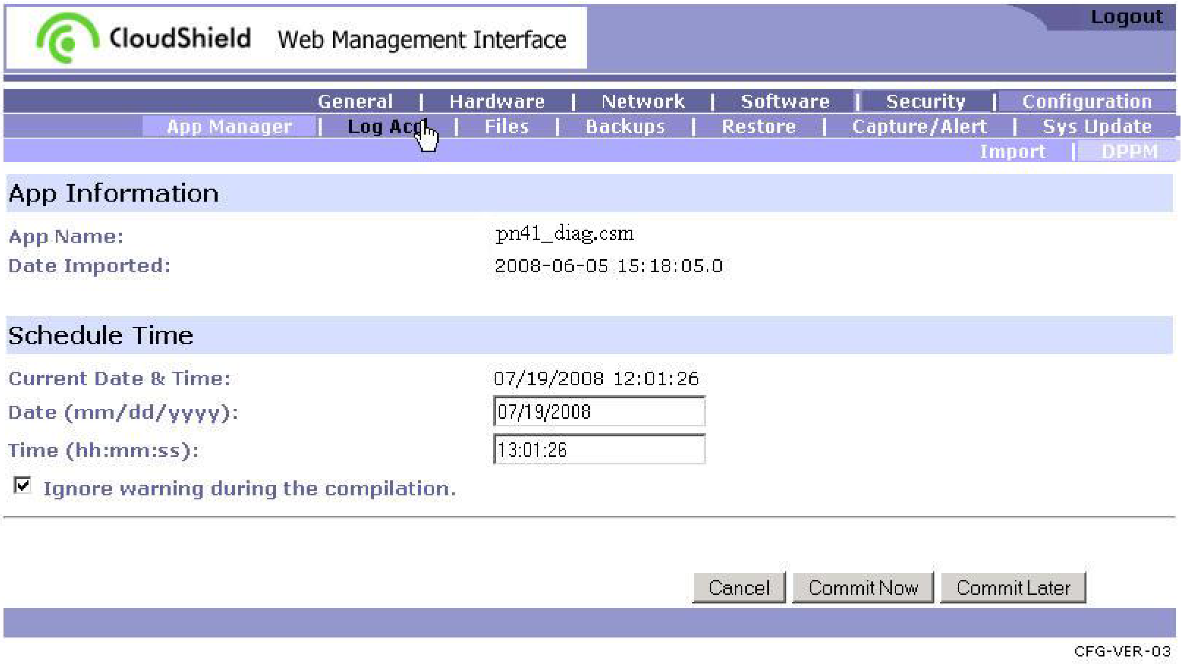
f. Select **Commit Now** or **Commit Later** to install the application to the DPI blade.

Notes:

1) The installation process can take up to 10 minutes.

2) The pn41_diag.csm application is the diagnostics application that comes with the DPI blade.

3) The drop_terminate.csm application also comes with the DPI blade. The drop_terminate application drops and terminates all packets that are received on an enabled port while the application is running.


CloudShield Web Management Interface
Logout
General | Hardware | Network | Software | Security | Configuration
App Manager | Log Acq | Files | Backups | Restore | Capture/Alert | Sys Update
Import | DPPM
Cancel
Commit Now
Commit Later
CFG-VER-03

App Information

App Name:	pn41_diag.csm
Date Imported:	2008-06-05 15:18:05.0

Schedule Time

Current Date & Time:	07/19/2008 12:01:26
Date (mm/dd/yyyy):	07/19/2008
Time (hh:mm:ss):	13:01:26

☑ Ignore warning during the compilation.

g. Click **OK** to complete the installation process.

Note: To view the variable statistics for the application, click the **Software** tab.

11. Enable networking ports on the DPI blade:
    a. In the Web Management Interface, click the **Hardware** tab.
    b. Enable the networking ports according to your installed applications.

Table 2. Networking ports

Switch-module bay	**DPI blade port**
	0 (front XFP)
7	1
8	3
9	2
10	4
	15 (front SFP)

c. Click the port that you want to enable and click **Modify**. Click **Enable**. Click **Update**.

For more information, see the CloudShield *Web Management Interface User Guide* and the CloudShield *Command Line Interface Reference Guide* on the IBM *Documentation* CD

First edition, August 2008

(1P) P/N: 44R5192