



APPENDIX **C**

Supporting and Using Additional CLI Access Options

The command line interface (CLI) management tool allows you to configure the MGX switches and display the switch status. When a switch starts up for the first time, the only CLI access available is through the console port (CP). After the switch is properly configured, you can access the CLI using any of the following:

- CP connection
- Terminal server connection
- Local LAN connection
- Dial-up connection
- ATM WAN connection

The following sections describe how to prepare the switch for the different types of CLI access and how to access the switch using these access methods.

Setting Up CP Port Connections

The Console Port (CP) connection requires no configuration on the switch. [Figure C-1](#) shows the hardware required for a console port connection to a PXM-UI-S3 back card.

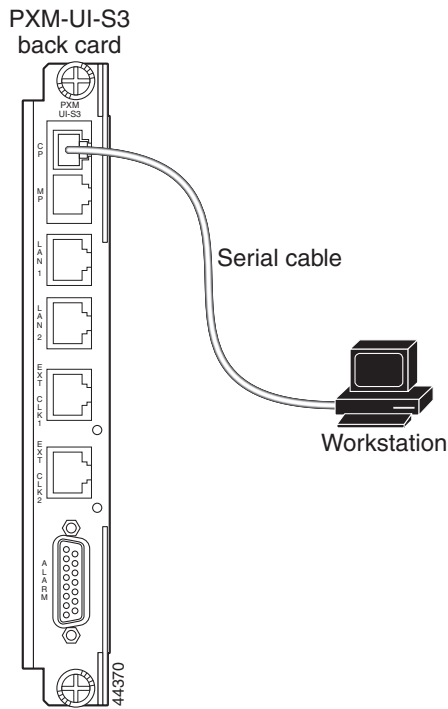
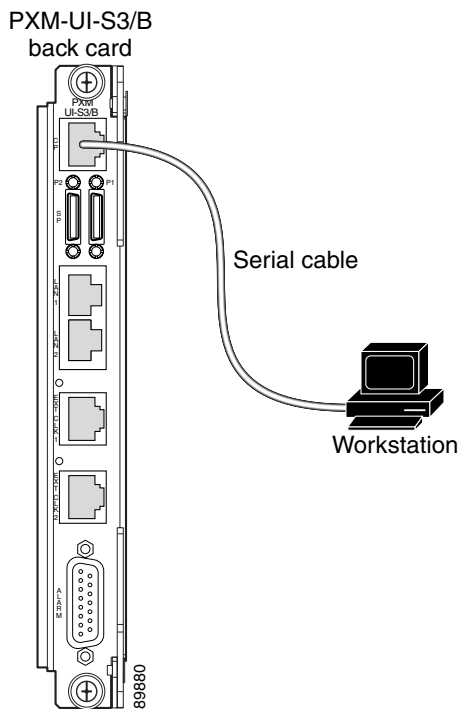
Figure C-1 Workstation Connection to the Console Port

Figure C-2 shows the hardware required for a console port connection to a PXM-UI-S3/B back card.

Figure C-2 Workstation Connection to Console Port on a PXM-UI-S3/B Back Card

The terminal you use should emulate a VT-100 terminal. You can use any personal computer or UNIX workstation and a terminal emulation program that emulates the VT-100.

The default switch configuration supports the following settings: 9600 bps, 8 data bits, no parity, 1 stop bit, no hardware flow control. The data rate of the interface can be configured for rates from 1200 to 38400 bps using the `cnfserialif` command.

Setting Up Terminal Server Connections

A terminal server connection allows remote access to the CP port. [Figure C-3](#) shows the hardware required for a terminal server connection.

Figure C-3 Terminal Server Connection to the Console Port on a PXM-UI-S3 Back Card

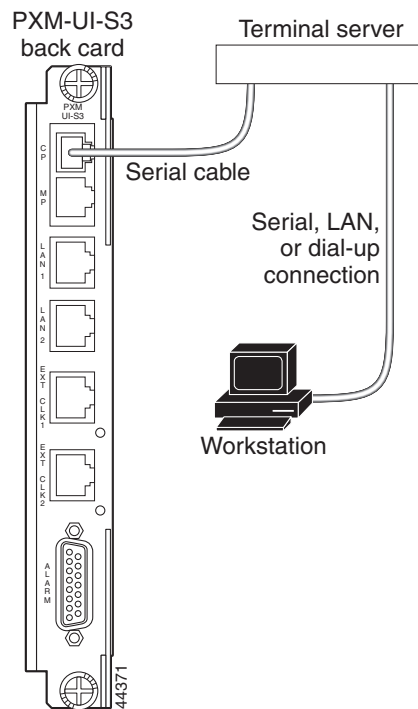
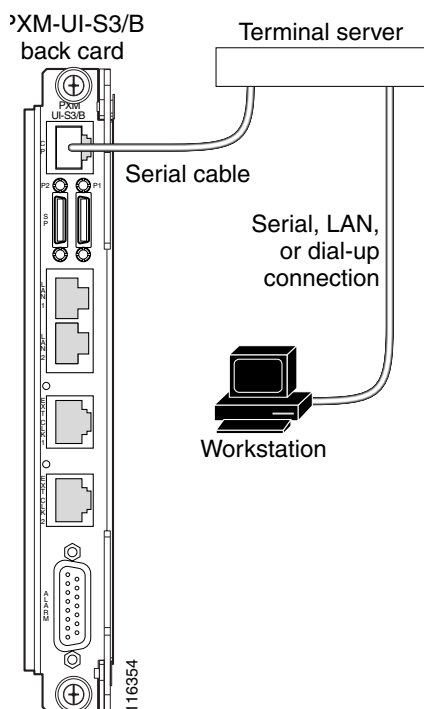


Figure C-4 shows the hardware required for a terminal server connection.

Figure C-4 Terminal Server Connection to the Console Port on a PXM-UI-S3/B Back Card



In the terminal server topology, any workstation with access to the terminal server can access the CP port as if the workstation were local. When the switch is operating properly, a terminal server connection offers no advantage over the other access methods. When the switch is not operating properly, however, other access methods might not function. In these situations, the CP port is more likely to operate than the other methods because it does not require IP connectivity to the workstation.

No special switch configuration is required to support a terminal switch configuration. The connection between the terminal server and the switch is a serial connection, which is the same as for a CP port connection. The following configuration tasks need to be completed at the terminal server:

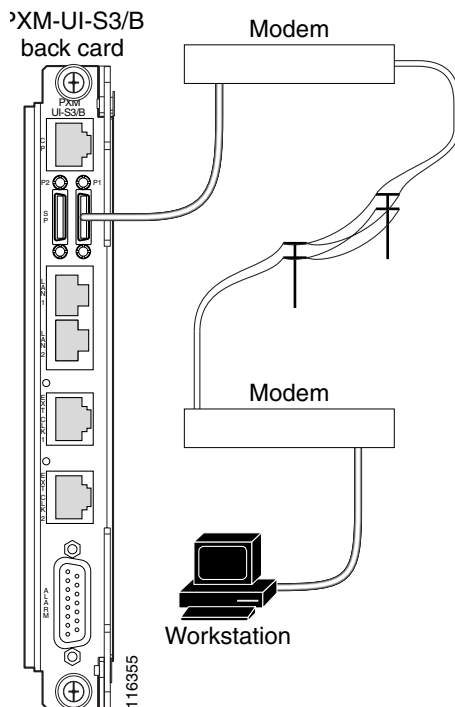
- The serial port to the switch must be enabled and configured.
- A second interface must be defined and configured for workstation access.

The workstation interface can be any interface type that both the workstation and the terminal server support. For example, the workstation interface could be an Ethernet interface for local LAN access, or it could be a dial-in interface for remote access.

To access the switch through the terminal server, the workstation establishes a connection to the terminal server using a terminal emulation program. After connecting to the terminal server, the workstation user enters a command that selects the serial port to the switch. Once the correct port is selected, the user logs in to the switch as if the user were using a CP port connection.

Figure C-6 shows the hardware required for a dial-up connection to a PXM1E UI-S3/B back card.

Figure C-6 Hardware Required for Dial-up Connections on a PXM-UI-S3/B Back Card



Before you can manage the switch using the dial-up interface, you must first assign an IP address to the maintenance port on the switch. This maintenance port is located on the PXM back card. For more information on physically connecting a modem to the maintenance port, refer to the *Cisco MGX 8800/8900 Hardware Installation Guide, Releases 2 - 5.2*.

To configure an IP address on the switch maintenance port, use the following procedure.

-
- Step 1** Establish a CLI management session using a username with SUPER_GP privileges. The default user name and password for this level are *superuser*, <*superuser*>.
- Step 2** Verify that the IP address is not already configured by entering the following command:

```
mgx8850a.7.PXM.a> dspif s10
```



Note If you omit the **s10** option, the switch displays the configuration for all switch IP interfaces: the ATM interface (atm0), the PXM LAN port interface (InPci0), and the PXM maintenance port interface (s10). Note that the address for each interface must be unique.

In the IP Interface Configuration Table, look for an Internet address entry under the **s10** entry. (You may need to press **Enter** to see this.) If an IP address is configured, you can use that address and skip the rest of this procedure. However, if the address has not been entered or is incompatible with your network, you must configure a valid IP address as described in the next step.

- Step 3** To set the IP address for the maintenance port, enter the **ipifconfig** command using the following format:
- ```
mgx8850a.7.PXM.a> ipifconfig s10 <IP_Addr> <netmask Mask>
```

Replace *<IP\_Addr>* with the IP address you want this port to use, and replace *<Mask>* with the network mask used on this network.



**Tip** Cisco recommends that you use the same subnet for all IP addresses defined on all MGX 8850 switches. This simplifies router configuration.



**Note** There are other options for the **ipifconfig** command, and you can set one or more options simultaneously. Any options you do not define in a command remain unchanged. For more information on this command, refer to the *Cisco MGX 8800/8900 Series Command Reference, Release 5.2*.

After you complete this procedure, the switch is ready for configuration through the maintenance port.

## Configuring the Switch

To support IP connectivity over the ATM interface, you need to do the following tasks:

1. Assign an IP address to the ATM interface.
2. Assign an AESA to the ATM interface.
3. Define an AESA for every adjacent router that supports IP communications to the ATM interface.
4. Configure ATM communications between the switch and the router.

To configure the switch to support IP connectivity to the ATM interface, use the following procedure.

**Step 1** Establish a CLI management session using a username with SUPER\_GP privileges. The default user name and password for this level are *superuser*, *<superuser>*.

**Step 2** Verify that the IP address for the ATM interface is not already configured by entering the following command:

```
mgx8850a.7.PXM.a> dspipif atm0
```



**Note** If you omit the **atm0** option, the switch displays the configuration for all switch IP interfaces: the ATM interface (atm0), the PXM LAN port interface (InPci0), and the PXM maintenance port interface (sl0). Note that the address for each interface must be unique.

In the IP Interface Configuration Table, look for an Internet address entry under the atm entry. If an IP address is configured, you can use that address. However, if the address has not been entered or is incompatible with your network, you must configure a valid IP address as described in the next step.

**Step 3** To set the switch IP address for the ATM interface, enter the **ipifconfig** command using the following format:

```
mgx8850a.7.PXM.a> ipifconfig atm0 <IP_Addr> <netmask Mask>
```

Replace *<IP\_Addr>* with the IP address you want this port to use, and replace *<Mask>* with the network mask used on this network.



**Note** Use a subnet mask that is different from the network mask used for LAN port communications. If you use the same subnet for both ATM and LAN port communications, there will be two entries for the same subnet in the routing table and all egress IP communications will take place through the atm0 port.



**Tip** Cisco recommends that you use the same subnet for all atm0 IP addresses defined on all MGX 8850 switches. This practice simplifies router configuration.



**Note** There are other options for the **ipifconfig** command, and you can set one or more options simultaneously. Any options you do not define in a command remain unchanged. For more information on this command, refer to the *Cisco MGX 8800/8900 Series Command Reference, Release 5.2*.

**Step 4** To verify the IP address you configured, enter the following command:

```
mgx8850a.7.PXM.a> dsppipif atm0
```

**Step 5** Make a note of the IP address defined for the atm0 interface. This is the IP address switch administrators must use to manage the switch.

**Step 6** Configure the switch AESA for IP connectivity by entering the following command:

```
mgx8850a.7.PXM.a> svcifconfig atm0 local <ATM_Addr>
```

Replace *ATM\_Addr* with the AESA for the interface. This address must conform to the address plan for the switch.

**Step 7** Define the AESA for the ATM router by entering the following command:

```
mgx8850a.7.PXM.a> svcifconfig atm0 router <ATM_Addr>
```

Replace *<ATM\_Addr>* with the AESA for the interface. This address must conform to the address plan for the switch.

**Step 8** To verify the ATM addresses you configured, enter the following command:

```
mgx8850a.7.PXM.a> dspsvcif
```

**Step 9** If you have not already done so, configure the PNNI controller as described in the “[Adding the PNNI Controller](#)” section in [Chapter 2, “Configuring General Switch Features.”](#)

**Step 10** Configure the ATM line to the ATM router as described in the “[PNNI UNI Port Configuration Quickstart](#)” section in [Chapter 3, “Provisioning PXM1E Communication Links.”](#)

The line configuration should specify a UNI port, SCT 6, and a partition that supports at least 20 connections.

**Step 11** To verify connectivity to directly attached ATM routers, enter the **dsppnsysaddr** command.

The ATM addresses of directly attached ATM routers should appear in the list the switch displays. To display an ATM address for a remote router, you need to establish a CLI session on the remote switch and enter the **dsppnsysaddr** command.

**Step 12** To check the status of ports leading to directly-attached ATM routers, enter the **dsppnports** command.



The following example shows commands that you can use to configure a Cisco MGX 8850 or MGX 8830 for IP communications over ATM.

### Example C-1 Switch Commands for IP Communications over ATM

```

mgx8850a.7.PXM.a> ipifconfig atm0 A.B.E.F # Replace A.B.E.F with IP Address
mgx8850a.7.PXM.a> svcifconfig atm0 local
47.0091.8100.0000.0010.7b65.f258.0010.7b65.1111.01
mgx8850a.7.PXM.a> svcifconfig atm0 router
47.0091.8100.0000.0010.7b65.f258.0010.7b65.ffff.f1
mgx8850a.7.PXM.a> addcontroller 2 i 2 7 #if controller does not already exist
mgx8850a.7.PXM.a> cnfcdsct 6
mgx8850a.7.PXM.a> upln 1.1
mgx8850a.7.PXM.a> addport 1 1.1 96000 96000 6 1
mgx8850a.7.PXM.a> addpart 1 1 2 500000 500000 500000 500000 1 20 32 52 1 20
mgx8850a.7.PXM.a> upport 1
mgx8850a.7.PXM.a> cnfilmi -if 1 -id 1 -ilmi 1 -vpi 0 -vci 16 -trap 1 -s 10 -t 10 -k 10
#Optional. This command configures ILMI for the port.
mgx8850a.7.PXM.a> addaddr 10:1.1:1 47.0091.8100.0000.0010.7b65.f258.0010.7b65.ffff.f1 160
#Enter only at switch with direct connection to router. Omit if using ILMI.
mgx8850a.7.PXM.a> dsppnsysaddr

```

(example output)

```

47.0091.8100.0000.0010.7b65.f258.0010.7b65.ffff/152
Type: uni Port id: 17111041

```

```

mgx8850a.7.PXM.a> dsppnports

```

(example output)

Per-port status summary

| PortId   | IF status | Admin status | ILMI state | Total Activeconns |
|----------|-----------|--------------|------------|-------------------|
| 10:1.1:1 | up        | up           | Undefined  | 3                 |

## Configuring the Router

To support IP over ATM communications on the ATM router, you need to configure the following interfaces:

- ATM interface to switch
- Interface to the LAN that hosts the management workstation

To configure the ATM interface to the switch, you need to do the following tasks:

- Create an ATM interface
- Assign an IP address to the ATM interface
- Assign an AESA to the ATM interface
- Configure the ATM interface to be the ATMARP server for the switch

If the router IP address for the ATM interface is on the same subnet as the IP address on the switch ATM interface, no additional configuration is required for the router IP LAN interface.

To configure the IP interface to the LAN, you need to do the following:

- If the router IP address for the ATM interface is not on the same subnet as the IP address on the switch ATM interface, you must manually configure on IP host-route for each MGX switch to which the interface will connect.

- Configure a routing protocol to broadcast the switch IP addresses to the LAN or create default routes to the switch on the management workstation.

The procedure you use to configure the ATM router will depend on the router you are using. The following example lists commands you can use on a Cisco router to support IP over ATM communications with the Cisco MGX switch.

**Example C-2 Router Configuration Commands for IP Communications over ATM**

```

config term
ip routing
ip route 0.0.0.0 0.0.0.0 W.X.Y.Z 1 (set default route)
interface atm 0
ip address A.B.C.D G.H.I.J # G.H.I.J = netmask
atm nsap-address 47.0091.8100.0000.0010.7b65.f258.0010.7b65.ffff.f1
atm uni-version 3.1
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi #Optional. Enter to enable ILMI.
atm ilmi-keepalive 10 #Optional. Enter to configure ILMI.
atm esi-address 00107B65FFFF.F1 #Optional. Enter to support ILMI.
atm arp-server self
no shut
^Z
write memory

```

## Starting a CLI Management Session Using a CP Port or Terminal Server Connection

The process for starting a CLI management session is similar for both CP port and terminal server connections. Both use a serial connection to the switch. The difference is that terminal server connections require that you first select the correct port at the terminal server.

After switch initialization, you can terminate and start sessions at any time using the terminal or workstation connection to the CP port or terminal server.

To start a CLI management session for CP port and terminal server connections, use the following procedure.

---

**Step 1** Turn on the terminal or start the terminal session.

For instructions on preparing the terminal and the connection, refer to the procedure in the previous section.

**Step 2** If you are accessing the switch through a terminal server, enter the commands that allow you to select the serial port that leads to the switch.

The following example shows the commands that accomplish this on a Cisco 2509-RJ Router.

```

User Access Verification

Password:
router>telnet 10.1.1.1 2001
Trying 10.1.1.1, 2001 ... Open

Login:

```

In the example above, the user first logs into the terminal server and then establishes a Telnet session to the terminal server using port 2001. All workstation communications pass through the Telnet server on the terminal server and out the serial connection designated by port 2001.



**Note** The built-in Telnet server on the switch, which is used by the other access methods, is not used for this type of connection.

- Step 3** If the Login prompt does not appear, press **Return**. The Login prompt comes from the switch and indicates that the terminal has successfully connected to the switch.
- Step 4** When the Login prompt appears, enter the login name supplied with your switch, and then enter the password for that login name. For example:

```
Login: superuser
password:

pop20one.7.PXM.a >
```

The switch does not display the password during login. When login is complete, the switch prompt appears, you have established a CLI management session, and you are ready to begin switch configuration and monitoring.

## Starting a CLI Telnet Session

Start a CLI Telnet session when you start a CLI management session using any of the following access methods, all of which require an IP address:

- Local LAN connection
- Dial-up connection
- ATM WAN connection

The switch includes a Telnet server process that you can use to connect to and manage the switch. Before you can establish a CLI Telnet session, you must set up the hardware for your access method and configure the switch as described earlier in the appendix.

After the appropriate interface has been configured and a physical path established to the MGX switch, you can start a CLI session using a workstation with a Telnet client program and the switch IP address. To establish a CLI management session, use the following procedure.

- Step 1** If you are dialing into the switch, establish a dial-up connection to the switch.
- You will need the telephone number for the line connected to the modem at the switch. For instructions on establishing the connection to the switch, refer to the documentation for the workstation and modem.
- Step 2** When the workstation has a path to the switch, start the Telnet program with a command similar to the following example:

```
C:>telnet <ipaddress>
```

Replace <ipaddress> with the IP address assigned to the switch. If the switch is configured to support multiple access methods, be sure to use the correct IP address for the access method you are using. For example, if you are using the local LAN access method, use the IP address configured for the InPCIO interface.




---

**Note** Note that the Telnet program on your workstation may require a different startup and connection procedure. For instructions on operating your Telnet program, refer to the documentation for that product.

---

**Step 3** If the Login prompt does not appear, press **Enter**.

The Login prompt comes from the switch and indicates that the workstation has successfully connected to the switch.

**Step 4** When the Login prompt appears, enter the user name provided with your switch and press **Enter**.

**Step 5** When the password prompt appears, enter the password provided with your switch and press **Enter**.

After you successfully log in, a prompt appears that is similar to the following example:

```
mgx8850a.7.PXM.a >
```

The switch does not display the password during login. When the login is complete, the switch prompt appears, you have established a CLI management session, and you are ready to begin switch configuration and monitoring.

---

## Starting a Secure (SSH) CLI Session

A secure CLI session uses the SSH protocol to encrypt all communications between a management workstation and the switch. This keeps the user ID, the password, and the details of your management session private.

Beginning with Release 5, Cisco MGX switches include an SSH server which is enabled by default. To establish a secure CLI session, you need to acquire SSH client software (which is not provided) and configure it for access to the server. The SSH secure session feature supports the following:

- Up to 12 simultaneous secure sessions on a switch
- Simultaneous SSH protocol version 1 (SSHv1) and version 2 (SSHv2) support
- Support for password authentication and public-key authentication
- Support for RSA (SSHv1) and DSA (SSHv2) key authentication algorithms
- Support for AES, 3DES, and Blowfish encryption methods
- Support for hmac-sha1 and hmac-md5 hashing methods
- SSH server support for accessing MGX CLI
- SSH client support for accessing remote SSH servers



**Tip**

---

For instructions on establishing a secure session between switches, see [“Starting and Managing Secure \(SSH\) Access Sessions Between Switches”](#) in Chapter 9, “Switch Operating Procedures.”

---

You can establish a secure CLI management session using any of the following access methods, all of which require an IP address:

- Local LAN connection
- Dial-up connection

- ATM WAN connection

Before you can establish a secure CLI management session, you must set up the hardware for your access method and configure the switch as described earlier in the appendix. After the appropriate interface has been configured and a physical path established to the MGX switch, you can start a secure CLI session using a workstation with a SSH client program and the switch IP address. To establish a CLI management session, use the following procedure.

**Note**

If your IP configuration supports it, you can establish a secure session with the active or the standby PXM. For more information, see “[Guidelines for Creating an IP Address Plan](#)” in [Chapter 1](#), “[Preparing for Configuration](#).”

---

**Step 1** If you are dialing into the switch, establish a dial-up connection to the switch.

You will need the telephone number for the line connected to the modem at the switch. For instructions on establishing the connection to the switch, refer to the documentation for the workstation and modem.

**Step 2** When the workstation has a path to the switch, start the SSH client program.

**Note**

The SSH client program requires that you enter the switch IP address, a user ID, and a password. Most client programs can store configurations so that future connections require that you select a configuration, click *Connect*, and enter your password. For details on how to configure and connect to an SSH server such as the Cisco MGX switch, refer to the documentation for your SSH client.

When you have successfully established a secure CLI session, the SSH client will display information similar to the following:

```
SSH Secure Shell 3.2.0 (Build 267)
Copyright (c) 2000-2002 SSH Communications Security Corp - http://www.ssh.com/
```

```
This copy of SSH Secure Shell is a commercial version
licensed to Cisco IT, Cisco Systems.
```

```
PXM1E_SJ.7.PXM.a >
```

**Step 3** If the switch prompt does not appear, press **Enter**.

The switch prompt comes from the switch and indicates that the workstation has successfully connected to the switch. When the SSH Secure Shell message appears with the switch prompt, you have established a secure CLI management session, and you are ready to begin switch configuration and monitoring.

---

## Ending a CLI Management Session

CLI management sessions automatically terminate after the configured idle time. The default idle time is 600 seconds (10 minutes) and can be changed with the **timeout** command. To end a CLI management session, enter the **bye** command.

**Note**

---

This command ends a CLI, SSH, or Telnet TCP session. It does not terminate the connection to the switch. For example, the **bye** command does not terminate a dial-up connection, a terminal server connection, a local LAN connection, or an ATM WAN connection. The connection remains in place until you terminate it using the terminal emulation software or Telnet client software. Some client software packages include commands to terminate the connection, and most client software packages close connections when you quit the program.

---

If you have not terminated a nonTCP connection after entering the **bye** command, you can restart a CLI management session by pressing **Return**. After you press **Return**, the switch prompts you for a username and password. The **bye** command terminates a TCP connection, so you must reestablish a TCP connection before you can restart a CLI management session.