

BLADE OS™

Release Notes

BNT 10-Port 10Gb Ethernet Switch Module for IBM BladeCenter®

Version 5.0

Part Number: BMD00091, June 2009

BLADE
NETWORK TECHNOLOGIES

2350 Mission College Blvd.
Suite 600
Santa Clara, CA 95054
www.bladenetwork.net

Copyright © 2009 BLADE Network Technologies, Inc., 2350 Mission College Blvd. Suite 600, Santa Clara, California, 95054, USA. All rights reserved. Reference number: BMD00091

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of BLADE Network Technologies, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct. 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct. 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct. 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov. 1995).

BLADE Network Technologies, Inc. reserves the right to change any products described herein at any time, and without notice. BLADE Network Technologies, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by BLADE Network Technologies, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of BLADE Network Technologies, Inc.

BLADE OS and BLADE are trademarks of BLADE Network Technologies, Inc. in the United States and certain other countries. Any other trademarks appearing in this manual are owned by their respective companies.

Originated in the USA.

Release Notes

The BNT 10-Port 10Gb Ethernet Switch Module (GbESM) is one of up to four GbESMs that can be installed in the IBM BladeCenter chassis.

These release notes provide the latest information regarding BLADE OS 5.0 for the BNT 10-Port 10Gb Ethernet Switch Module. This supplement modifies information found in the complete documentation:

- *BLADE OS 5.0 Application Guide* for the BNT 10-Port 10Gb Ethernet Switch Module for IBM BladeCenter
- *BLADE OS 5.0 Command Reference* for the BNT 10-Port 10Gb Ethernet Switch Module for IBM BladeCenter
- *BLADE OS 5.0 ISCLI Reference* for the BNT 10-Port 10Gb Ethernet Switch Module for IBM BladeCenter
- *BLADE OS 5.0 BBI Quick Guide* for the BNT 10-Port 10Gb Ethernet Switch Module for IBM BladeCenter
- BNT 10-Port 10Gb Ethernet Switch Module for IBM BladeCenter, *Installation Guide*

The publications listed above are available from the IBM support website:

<http://www.ibm.com/systems/support>

Please keep these release notes with your product manuals.

Hardware Support

This BLADE OS software is supported only on the BNT 10-Port 10Gb Ethernet Switch Module (GbESM) for IBM BladeCenter. The GbESM is a high performance Layer 2/3 embedded network switch that features tight integration with the IBM BladeCenter H or BladeCenter HT management module. The GbESM has ten 10Gbps external ports (see [Figure 1](#)). The number and type of ports are as follows:

- Ten 10Gbps SFP+
- Fourteen 10Gb internal ports
- One 1Gb external copper (RJ-45)
- Two 100Mb internal management ports
- One RS-232 serial port

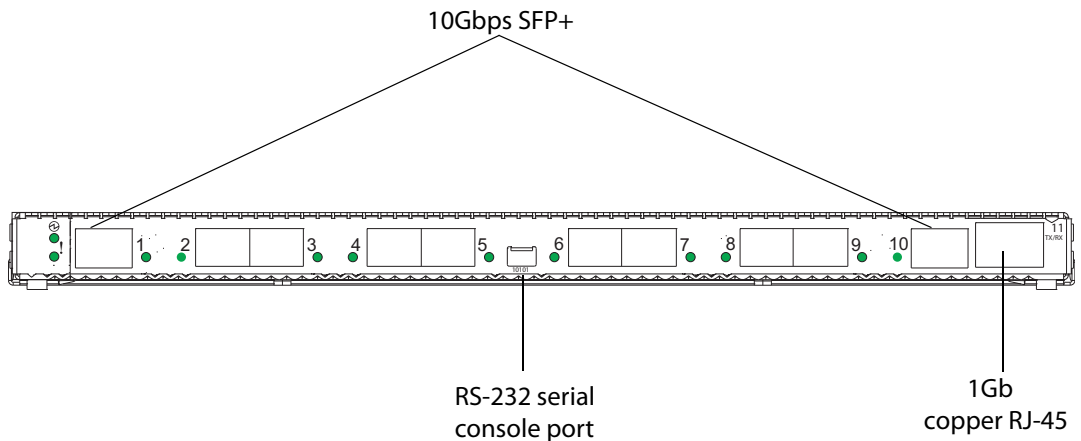


Figure 1 BNT 10-Port 10Gb Ethernet Switch Module Faceplate

Updating the Switch Software Image

The switch software image is the executable code running on the GbESM. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software available for your GbESM, go to:

<http://www.ibm.com/systems/support>

From the Blade OS CLI, use the `/boot/cur` command to determine the current software version.

The typical upgrade process for the software image consists of the following steps:

- Place the new image onto a FTP or TFTP server on your network, or on a local computer.
- Transfer the new image to your switch.
- Select the new software image to be loaded into switch memory the next time the switch is reset.

Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

To download a new software image to your switch, you will need the following:

- The image or boot software loaded on a FTP or TFTP server on your network
- The hostname or IP address of the FTP or TFTP server
- The name of the new software image or boot file

Note – The DNS parameters must be configured if specifying hostnames.

Image Names

- Image file: `GbESM-24-10G-5.0.1.0_OS.img`
- Boot file: `GbESM-24-10G-5.0.1.0_Boot.img`

When the above requirements are met, use one of the following procedures to download the new software to your switch. You can use the Blade OS CLI, the ISCLI, or the BBI to download and activate new software.

Note – When performing this update, be sure to download the new boot file and the new image file.

Using the Blade OS CLI

1. At the `Boot Options#` prompt, enter:

```
Boot Options# gting
```

2. Enter the name of the switch software to be replaced:

```
Enter name of switch software image to be replaced  
["image1"/"image2"/"boot"]: <image>
```

3. Enter the hostname or IP address of the FTP or TFTP server.

```
Enter hostname or IP address of FTP/TFTP server: <name or IP address>
```

4. Enter the name of the new software file on the server.

```
Enter name of file on FTP/TFTP server: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (usually `/tftpboot`).

5. Enter your username for the server, if applicable.

```
Enter username for FTP server or hit return for TFTP server: <username>  
or <Enter>
```

6. The system prompts you to confirm your request.

After loading software to the switch, select a software image to run, as described below.

Use the following procedure to select which OS software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

7. At the `Boot Options#` prompt, enter:

```
Boot Options# image
```

8. Enter the name of the image you want the switch to use upon the next boot.

The system informs you of which image is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use switch software "image1" on next reset.  
Specify new image to use on next reset ["image1"/"image2"]:
```

Using the ISCLI

1. In Privileged EXEC mode, enter the following command:

```
Router# copy {tftp|ftp} {image1|image2|boot-image}
```

Select a port, or press <Enter> to use the default (management port).

2. Enter the hostname or IP address of the FTP or TFTP server.

```
Address or name of remote host: <name or IP address>
```

3. Enter the name of the new software file on the server.

```
Source file name: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (usually `tftpboot`).

4. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

5. The system prompts you to confirm your request.

After loading software to the switch, select a software image to run, as described below.

Use the following procedure to select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

6. In Global Configuration mode, enter:

```
Router(config)# boot image {image1|image2}
```

7. Enter the name of the image you want the switch to use upon the next boot.

The system informs you of which image set to be loaded at the next reset:

```
Next boot will use switch software image1 instead of image2.
```

Using the BBI

You can use the Browser-Based Interface to load software onto the GbESM. The software image to load can reside in one of the following locations:

- FTP server
- TFTP server
- Local computer

After you log onto the BBI, perform the following steps to load a software image:

1. Click the Configure context tab in the toolbar.
2. In the Navigation Window, select System > Config/Image Control.

The Switch Image and Configuration Management page appears.

| Switch Image and Configuration Management | | | | | | | | | |
|---|--|----------------------------|----------------|---|------------------|--|---|---------------------------------|--|
| Image 1 Version | version 5.0.0, downloaded 22:18:01 Tue Jan 25, 2008 NormalConnect | | | | | | | | |
| Image 2 Version | version 5.0.2, downloaded 21:23:44 Mon Jan 24, 2008 NormalConnect | | | | | | | | |
| Boot Version | version 5.0.0 | | | | | | | | |
| Active Image Version | 5.0.2 | | | | | | | | |
| Next Boot Image Selection | image 2 ▾ | | | | | | | | |
| <table border="1"> <tr> <td>Active Configuration Block</td> <td>factory config</td> </tr> <tr> <td>Next Boot Configuration Block Selection</td> <td>factory config ▾</td> </tr> <tr> <td>Next CLI Boot Mode Selection</td> <td>BLADEOS CLI ▾</td> </tr> <tr> <td>Prompt for selectable boot mode</td> <td>ENABLE ▾</td> </tr> </table> | | Active Configuration Block | factory config | Next Boot Configuration Block Selection | factory config ▾ | Next CLI Boot Mode Selection | BLADEOS CLI ▾ | Prompt for selectable boot mode | ENABLE ▾ |
| Active Configuration Block | factory config | | | | | | | | |
| Next Boot Configuration Block Selection | factory config ▾ | | | | | | | | |
| Next CLI Boot Mode Selection | BLADEOS CLI ▾ | | | | | | | | |
| Prompt for selectable boot mode | ENABLE ▾ | | | | | | | | |
| <table border="1"> <tr> <td colspan="2"><u>FTP/TFTP Settings</u></td> </tr> <tr> <td>Hostname or IP Address of FTP/TFTP server</td> <td>100.10.20.1</td> </tr> <tr> <td>Username for FTP Server or Blank for TFTP Server</td> <td></td> </tr> <tr> <td>Password for FTP Server</td> <td></td> </tr> </table> | | <u>FTP/TFTP Settings</u> | | Hostname or IP Address of FTP/TFTP server | 100.10.20.1 | Username for FTP Server or Blank for TFTP Server | | Password for FTP Server | |
| <u>FTP/TFTP Settings</u> | | | | | | | | | |
| Hostname or IP Address of FTP/TFTP server | 100.10.20.1 | | | | | | | | |
| Username for FTP Server or Blank for TFTP Server | | | | | | | | | |
| Password for FTP Server | | | | | | | | | |
| <table border="1"> <tr> <td colspan="2"><u>Image Settings</u></td> </tr> <tr> <td>Image for Transfer</td> <td>image 1 ▾</td> </tr> <tr> <td>Image Filename (on server)</td> <td>5.0.2_OS.img Get Image Put Image</td> </tr> <tr> <td>Image Filename (on HTTP Client)</td> <td><input type="text"/> Browse... Download via Browser</td> </tr> </table> | | <u>Image Settings</u> | | Image for Transfer | image 1 ▾ | Image Filename (on server) | 5.0.2_OS.img Get Image Put Image | Image Filename (on HTTP Client) | <input type="text"/> Browse... Download via Browser |
| <u>Image Settings</u> | | | | | | | | | |
| Image for Transfer | image 1 ▾ | | | | | | | | |
| Image Filename (on server) | 5.0.2_OS.img Get Image Put Image | | | | | | | | |
| Image Filename (on HTTP Client) | <input type="text"/> Browse... Download via Browser | | | | | | | | |

3. If you are loading software from your computer (HTTP client), go to step 4. Otherwise, if you are loading software from a FTP/TFTP server, enter the server's information in the FTP/TFTP Settings section.
4. In the Image Settings section, select the image version you want to replace (Image for Transfer).
 - If you are loading software from a FTP/TFTP server, enter the file name and click **Get Image**.
 - If you are loading software from your computer, click **Browse**.

In the File Upload Dialog, select the file and click **OK**. Then click **Download via Browser**.

Once the image has loaded, the page refreshes to show the new software.

Software features

The list of features below briefly summarizes the functionality of the BNT 10-Port 10Gb Ethernet Switch Module (GbESM) in BLADE OS 5.0.

For more detailed information about configuring GbESM features and capabilities, refer to the *BLADE OS 5.0 Application Guide*.

Switch Management

- IBM management module integration
- BladeCenter Enterprise (BCH) and Telco (BCHT) chassis support
- Browser-Based Interface (HTTP and HTTPS)
- Telnet support
- SSH/SCP support (version 1 and version 2)
- RADIUS authentication and authorization
- TACACS+ authentication and authorization
- LDAP authentication
- SNMP v1/v2c and v3 support
- FTP/TFTP image and configuration management
- Scriptable configuration management
- Protected mode

Layer 2

- 1024 Virtual LANs (VLANs)
 - VLAN Tagging
 - Protocol-based VLANs
 - Private VLANs
- Spanning Tree Protocol
- Rapid Spanning Tree Protocol and Multiple Spanning Tree Protocol
- PVST+ compatibility
- Trunking (port channel/port aggregation)
- Link Aggregation Control Protocol (LACP)

- Layer 2 Trunk Failover
- 802.1X Port Authentication (EAPOL)
- QoS/ACL Layer 2 Filtering
- 802.1p/Class Of Service support
- Fast Uplink Convergence

Layer 3

- 128 IP Interfaces
- IPv6 host management
- IP Routing
- Inter-VLAN routing
- 128 IPv4 static routes
- RIP v1 and v2
- OSPFv2
- BGPv4
- Differentiated Services
- IGMP Snooping, v1, v 2, and v3
- IGMP Relay

High Availability

- Virtual Router Redundancy Protocol (VRRP)
- Active-Active support

Security

- Broadcast Storm Control
- Secure switch administration

Supplemental Information

This section provides additional information about configuring and operating the GbESM and BLADE OS.

Management Module

- The “Fast POST=Disabled/Enabled” inside the IBM management module Web interface “I/O Module Admin Power/Restart” does not apply to the GbESM.

Solution: To boot with Fast or Extended POST, go to the “I/O Module Admin/Power/Restart” window. Select the GbESM, and then choose “Restart Module and Run Standard Diagnostics” or “Restart Module and Run Extended Diagnostics.”

- The following table correlates the Firmware Type listed in the IBM management module’s Web interface “Firmware VPD” window to the GbESM software version:

Table 1 Firmware Type list

| Firmware Type | Description |
|--------------------|-------------------------|
| Boot ROM | GbESM Boot code version |
| Main Application 1 | Currently running image |
| Main Application 2 | Backup image |

- Within the IBM management module Web interface, the Java applets of “Start Telnet Session” and “Start Web Session” do not support changing of default known ports 23 and 80 respectively.

Solution: If the Telnet or HTTP port on the GbESM is changed to something other than the default port number, the user must use a separate Telnet client or Web browser that supports specifying a non-default port to start a session to the GbESM user interface.

Management Module/GbESM Connectivity

Currently, the IBM management module is designed to provide one-way control of the GbESM. As a result, the GbESM may lose connectivity to the management module via the management port under the following conditions:

- If new IP attributes are pushed from the management module to the GbESM while the IP Routing table is full, the new attributes will not be applied.

Solution: Enable “External Management over all ports,” connect to the switch using other interface and then clear the routing table. Then push the IP address from the management module. If this does not work, use Solution 2 below.

- If you execute the `/boot/reset` CLI command on the GbESM or the GbESM resets itself, the management module might not push the IP attributes to the switch, and connectivity may be lost.

Solution 1: If you should experience any connectivity issues between the switch module and the management module, go to the “I/O Module Configuration” window on the management module’s Web interface. Under the “New Static IP Configuration” section, click **Save** to trigger the management module to push the stored IP attributes to the switch module.

Solution 2: If Solution 1 does not resolve your connectivity issue, then go to the “I/O Module Admin/Power/Restart” window on the management module’s Web interface. Restart the switch module in question.

Solution 3: If this still does not resolve the issue, enable Preserve new IP configuration on all resets setting on the management module and restart the switch module via the “I/O Module Admin/Power/Restart” window on the management module’s Web interface.

Note – As a rule, always use the management module Web interface to change the GbESM management IP attributes (IP address, mask and gateway), and then click **Save** to push the IP attributes to the switch module. Use of the command-line interface to change the switch module management IP attributes may result in duplicated IP Interface 250 entries in the switch route table and/or loss of connectivity via the management module.

Secure Management Network

The following GbESM attributes are reserved to provide secure management access to and from the IBM management module:

- Internal management
 - MGT1 (port 15) and MGT2 (port 16)
 - VLAN 4095
 - IP interface 128
 - Gateway 132
 - For more information about remotely managing the GbESM through the external ports, see “Accessing the Switch” in the *BLADE OS 5.0 Application Guide*.

Note – The external uplink ports (EXTx) cannot be members of the management VLAN (4095).

Secure Shell (SSH)

Because SSH key generation is CPU intensive, the GbESM attempts to avoid unnecessary key generation. The process generates three server keys:

1. One key is generated to replace the current server key, if used.
2. A second key is generated as a spare, in case the current server key is used and the specified interval expires.
3. A third key is generated for use at the next reboot.

Therefore, if you never login via SSH, you will only see two key generation events. You may see all three events directly following a reboot. If you want to witness the key generation after the specified interval has expired, then you must login via SSH at least once during each expiration interval.

Port Mirroring Tags BPDUs Packets

When you perform port mirroring, Spanning Tree BPDUs packets are VLAN tagged at the monitoring port. This is standard behavior of port mirroring on the GbESM. All mirrored egress traffic is tagged.

Trunk Group Configuration Tips

Please be aware of the following information when you configure trunk groups:

- Always configure trunk groups first on both ends, before you physically connect the links.
- Configure all ports in a trunk group to the same speed.

Spanning Tree Configuration Tips

To ensure proper operation with switches that use Cisco Per VLAN Spanning Tree (PVST+), you must do one of the following:

- Create a separate Spanning Tree Group for each VLAN.
- Manually add all associated VLANs into a single Spanning Tree Group.

Syslog Configuration Tip

The *facility* parameter traditionally is used to correlate services (e.g. IP, CLI, etc.) to messages. This is done to distinguish between the different services that are running in the network/device. However, for the GbESM, there is a single configured facility value (0-7) used on all messages. By configuring a unique facility value for each switch, a single SYSLOG server can distinguish between the various GbESMs in the network. Refer to “System Host Log Configuration” in the *BLADE OS 5.0 Command Reference*.

Internal Port Autonegotiation

By default, link autonegotiation is turned on for internal ports. This is in contrast to external ports, where autonegotiation is off by default. Internal ports use autonegotiation in order to support the Wake-Over-LAN (WOL) features of some servers. If an attached server does not support autonegotiation or WOL, turn autonegotiation off for the internal port.

VRRP Configuration

Although the Virtual Router Redundancy Protocol (VRRP) standard permits Virtual Router IDs (VRIDs) between 1 and 255, the BLADE OS 5.0 implementation allows the configuration of VRIDs between 1 and 128, corresponding to the number of supported IP interfaces.

Known issues

This section describes known issues for BLADE OS 5.0 on the BNT 10-Port 10Gb Ethernet Switch Module.

Jumbo Frames

Some ingress jumbo frames (for example, ICMP) are not routed from one VLAN to another VLAN. Jumbo frames are routed across data VLANs.

ACL Filtering

When an ACL is installed on two different ports, only one statistics counter will be available. The GbESM does not support two different statistics counter for one ACL installed on two different ports.

Link Aggregation Control Protocol

If a static trunk on a GbESM is connected to another GbESM with LACP configured (but no active LACP trunk), the `/info/12/trunk` command might erroneously report the static trunk as forwarding.

If you configure LACP (active/passive) on one port, also configure LACP on the partner switch, at the end of the link. If you connect LACP with a static trunk, there will be no connectivity on that link.

ACL Filters

The ACL filters for TCP/UDP work properly only on packets that do not have IP options.

QoS Metering

Traffic may exceed the configured maximum burst size of the ACL meter (`/cfg/port x/aclqos/meter/mbsize`) by one packet, with that packet remaining In-Profile. Once the ACL meter has been exceeded, additional burst packets fall Out-of-Profile.

QoS and Trunking

When you assign an ACL (or ACL Group) to one port in a trunk, BLADE OS does not automatically assign the ACL to other ports in the trunk, and it does not prompt you to assign the ACL to other ports in the trunk.

Solution: Manually assign each ACL or ACL Group to all ports in a trunk.

RIP MIBs

Due to backward-compatibility issues, two Routing Information Protocol (RIP) MIBs are available in BLADE OS: `ripCfg` and `rip2Cfg`. Use the `rip2Cfg` MIB to configure RIPv1 and RIPv2 through SNMP.

BLADE OS does not support the standard RIPv2 MIB, as described in RFC 1724. Use the `rip2Cfg` MIB to configure RIPv1 and RIPv2 through SNMP.

Trunk and Link Loop

When you create a trunk or link loop between the GbESM and another switch, packets might loop infinitely at line rate within the related links. When this problem occurs, the GbESM continuously displays the following messages at the console:

```
WARNING: packet_sent u: 0, dv_active: tx ring full
packet_sent dcnt=114, public1=110, vcnt=1025
```

Solution: Remove the loop to resolve this misconfiguration.

Browser Based Interface

- Some versions of Microsoft Internet Explorer version 6.x do not perform HTTP download efficiently. If you have one of these versions, HTTP software download might take much longer than expected (up to several minutes).
- Web-browsers from different vendors may vary in their support of standard features. If you encounter problems using the BBI in a particular browser, a different browser may resolve the issue.

GMT Displayed While Booting

While the switch is booting, the system time may be displayed for GMT (time zone 0) in the System Log. However, once the switch has finished booting, the administrator-configured time zone will be used for subsequent log messages.

Blocking Egress Traffic

Access Control Lists (ACLs) which are configured to match both a destination MAC address and an egress port fail to act when the matching packets are encountered. As a result, ACLs cannot be used to block traffic exiting specific ports for specific static multicast MAC addresses.

Solution: Instead of using an ACL to block the traffic, configure a static multicast route that includes all ports other than those you wish to block. Consider an example where you wish to block port EXT1 for DMAC 01:02:03:04:05:FF on the default VLAN (VLAN 1). In this case, you would add a multicast route that includes all ports except EXT1. For example:

```
# /cfg/12/fdb/mcast/add <Destination MAC> <VLAN> <list of ports or ranges to allow>
or
# /cfg/12/fdb/mcast/add 01:02:03:04:05:FF 1 INT1-INT14 EXT2-EXT10
```

Changing Port Transceivers

Under repeated and rapid removal and reinsertion a port transceiver, it is possible that the resulting port state may not be represented accurately within the switch.

Solution: Once you have removed a transceiver from a switch port, wait five seconds before reinserting any transceiver into the same port. This allows the port to stabilize, and promotes accurate port state information within the switch.

TACACS+ Passwords

Changing the TACACS+ password for the secondary TACACS+ authentication server causes the authentication to failover from the primary authentication server to the secondary. Subsequent authentication attempts fail when using the primary server password and succeed when using the secondary server password.

Solution: To avoid confusion, set the primary authentication server to use the same password as the secondary server prior to applying the configuration.

ISCLI Configuration Scripts

When using the ISCLI, configuration commands are applied to the active switch configuration immediately upon execution. As a result, when using the ISCLI to load a configuration script containing a long list of processor-intensive commands (such as static route definitions), switch response to other management functions (such as Telnet access for additional management sessions) may be slow or even time-out while the switch individually applies each scripted command.

Solution: The CLI may be used as an alternative to the ISCLI. Because CLI commands are not fully processed until the CLI `apply` command is given, the equivalent configuration script can be loaded in its entirety and then applied as a whole without undue impact on other management sessions.

