Whitepaper

Enabling and Configuring SOL (Serial Over LAN) on an 8839 Blade Server

Written By: Mike Nolterieke

Revision Level: 06
Last Revised: 7/18/2005 9:55 AM

I. Introduction

This white paper explains how to update and configure the various BladeCenter modules and 8839 Blade Server components used to enable Serial Over LAN, herein referred to as SOL.

There are several BladeCenter modules and 8839 Blade Server components that must be updated and configured correctly in order for SOL to function properly. This white paper details which modules and components are necessary and the steps to update and configure them properly. It is very important that all of the steps outlined in this document are carefully followed to enable SOL functionality.

This white paper was written for use with the IBM BladeCenter 1.0 chassis, IBM 4-Port Gigabit ESM (Ethernet Switch Module), Nortel Networks 4-Port Layer 2-7 Gigabit ESM (Ethernet Switch Module), Nortel Networks 6-Port Layer 2-3 Gigabit ESM (Ethernet Switch Module), Cisco Systems Intelligent Gigabit ESM (Ethernet Switch Module), 8839 Blade Server(s), Red Hat Enterprise Linux ES 2.1, and SUSE SLES 8.0.

Notes:

This whitepaper provides instructions for updating and configuring the IBM 4-Port Gigabit ESM (Ethernet Switch Module), Nortel Networks 4-Port Layer 2-7 Gigabit ESM (Ethernet Switch Module), Nortel Networks 6-Port Layer 2-3 Gigabit ESM (Ethernet Switch Module), and the Cisco Systems Intelligent Gigabit ESM (Ethernet Switch Module). These are the only ESM's that currently support SOL. The terms "IBM ESM", "Nortel ESM", "Cisco ESM", and "ESM" will be used for the rest of this document to refer to the IBM 4-Port Gigabit, Nortel Networks 4-Port Layer 2-7 Gigabit, Nortel Networks 6-Port Layer 2-3 Gigabit, and Cisco ESM's unless otherwise specifically stated.

The SOL VLAN (Virtual Local Area Network) ID is an internal virtual network that the MM (BladeCenter Management Module) and ESM's use for SOL communications. This parameter is configurable and is different depending on which ESM you have installed. If you have either an IBM or Nortel ESM, the value of this parameter must be 4095. If you have a Cisco ESM, this parameter cannot be 4095. For the Cisco ESM, any value from 3 - 1001 is acceptable. You must ensure that the SOL VLAN ID for the MM and your ESM match and are the correct values.

In order for SOL to function properly, a supported ESM must be installed in the I/O Module Bay 1 of the BladeCenter chassis.

Technical Limitations:

There are no currently known technical limitations.

II. SOL Overview

SOL is accomplished in the following way: Serial data that flows to and from the 8839 Blade Server(s) COM port is routed through the network infrastructure of the BladeCenter chassis. This network infrastructure includes the BladeCenter Management Module, the ESM (Ethernet Switch Module), and the onboard NIC (Network Interface Controller) of the 8839 Blade Server(s). In addition the 8839 Blade Server(s) BMC (Baseboard Management Controller) also assists in handling the serial data to and from the COM port. The BladeCenter Management Module acts as a proxy in the network infrastructure to couple a client running a telnet session to the BladeCenter Management Module with an SOL session to the 8839 Blade Server(s). This then allows the telnet client to interact with the serial port of the 8839 Blade Server over the network.

Since all of the SOL traffic is controlled by and routed through the BladeCenter Management Module, it is possible for administrators to segregate the management traffic of the BladeCenter from the data traffic of the Blade Server(s).

In order to initiate an SOL connection to an 8839 Blade Server, you must first establish a telnet CLI (Command Line Interface) session to the BladeCenter Management Module. Once the telnet CLI session to the BladeCenter Management Module has been established, you can then initiate a remote console SOL session to any individual 8839 Blade Server. You can establish as many as 20 separate telnet sessions to one BladeCenter Management Module. This gives you the ability to have a maximum of one SOL session active on all 14 8839 Blade Server(s) at the same time and also have 6 additional CLI sessions for BladeCenter chassis management. If security is a concern, SSH (Secure Shell) sessions are also available so users can establish secured telnet CLI sessions to the BladeCenter Management Module prior to starting an SOL console redirect session to the 8839 Blade Server(s).

Notes:

The 8839 Blade Server requires the global SOL settings, “Accumulate timeout” and “Retry interval”, to be higher than the default values. These new values will not affect the operation of SOL other Blades in the same chassis.

Telnet sessions with the BladeCenter management module have a default timeout value of 120 seconds (2 minutes). If there is no Telnet or SOL traffic within the timeout interval, the Telnet session and any SOL session associated with this Telnet session will terminate. See the *IBM Eserver BladeCenter Management Module Command-Line Interface Reference Guide* for information about configuring the Telnet session timeout value.

Due to the encryption of data on an SSH session there will be some performance impact as seen by the remote SSH client.

III. SOL BladeCenter Modules and 8839 Blade Server Components

Below is a table of BladeCenter modules and 8839 Blade Server components required to enable SOL. The latest updates for these modules and components should be obtained from the IBM web site prior to following the instructions outlined in this document.

BladeCenter Management Module
8839 Blade Server BMC
8839 Blade Server BIOS
8839 Blade Server Intel Ethernet Controller Linux Device Driver
IBM 4-Port Gigabit ESM (Ethernet Switch Module)
Nortel Networks 4-Port 2-7 Layer ESM (Ethernet Switch Module)
Nortel Networks 6-Port 2-3 Layer ESM (Ethernet Switch Module)
Cisco Systems Intelligent Gigabit ESM (Ethernet Switch Module)

IV. BladeCenter Management Module

The following assumptions have been made for these directions

1. The BladeCenter Management Module External Network Interface (eth0) already has a valid configuration for your production network
2. You are able to and have already connected to the BladeCenter Management Module Web interface

The following considerations must to be taken into account prior to configuring the network settings to enable SOL.

The BladeCenter Management Module External Network Interface (eth0) configuration must have a valid configuration for your production network. This configuration may be obtained from a DHCP server or set statically.

The BladeCenter Management Module Internal Network Interface (eth1) and the ESM configuration can be different than that of the BladeCenter Management Module External Network Interface (eth0). However, the BladeCenter Management Module Internal Network Interface (eth1) and the ESM configuration must reside the within the same subnet. Keep in mind that the BladeCenter Management Module Internal Interface (eth1) is exposed to the external network via the BladeCenter Management Module so the configuration used must not conflict with other addresses on your production network. Also, if you use a configuration for the ESM that is not valid for your production network, you will not be able to update the firmware or manage your ESM via the telnet or Web interfaces.

The SOL BSMP (Blade System Management Processors) address range can be anything you wish as long as it does not conflict with any of the actual IP addresses of the 8839 Blade Servers. These addresses are used for internal communications only and are not exposed to the external network.

Below is the configuration that was used during the development of this document and will be used as reference and examples.

BladeCenter Management Module External Network Interface (eth0)

IP address:	9.xxx.xxx.173
Subnet mask:	255.255.255.128
Gateway address:	9.xxx.xxx.129

Note: The configuration above was obtained from a DHCP server on the production network

BladeCenter Management Module Internal Network Interface (eth1)

IP address:	9.xxx.xxx.151
Subnet mask:	255.255.255.128
Gateway address:	9.xxx.xxx.129

ESM

IP address:	9.xxx.xxx.147
Subnet mask:	255.255.255.128
Gateway address:	9.xxx.xxx.129

SOL BSMP

BSMP IP address range:	10.1.1.100

Follow the directions outlined below to update the firmware and configure the BladeCenter Management Module to enable SOL.

1. Update the BladeCenter Management Module firmware
    a. Obtain the latest BladeCenter Management Module zip file
    b. Unzip the file obtained above into a temporary directory
    c. Update the BladeCenter Management Module firmware
        Note: There are three packet files (cnet??us.pkt) required to update the firmware of the BladeCenter Management Module. You must repeat the steps below for each of the packet files
        i. Click on the "Firmware Update" link in the "MM Control" section
        ii. Click the "Browse…" button in the "Update MM Firmware" section
        iii. Select one of the firmware files that has a ".pkt" extension from the temporary directory where you unzipped the latest build in step b above and click the "Open" button
        iv. Click the "Update" button in the "Update MM Firmware" section and wait for the status window to close
        v. Click the "Continue" button in the "Confirm Firmware Update" section and wait for the update to complete
        Repeat these steps for the remaining firmware packet files
    d. Restart the BladeCenter Management Module
        Do not restart the BladeCenter Management Module until you have completed the steps above for ALL of the firmware packet files
        i. Click on the "Restart MM" link in the "MM Control" section
        ii. Click the "Restart" button in the "Restart MM" section
        iii. Click the "OK" button in the confirmation window
        iv. Click "Yes" to close the current Web interface
        v. Wait about 30 seconds or so, start a new Web browser, and reconnect to the BladeCenter Management Module Web interface
2. Configure the BladeCenter Management Module to enable SOL
    a. Configure the "Internal Network Interface (eth1)" settings
        i. Click on the "Network Interfaces" link in the "MM Control" section
        ii. Ensure that the "Enabled" option is selected for the "Interface" field in the "Internal Ethernet Interface (eth1)" section
        iii. Set and save the "Static IP Configuration" fields in the "Internal Network Interface (eth1)" section
            1. Set the "IP address" (9.xxx.xxx.151)
            2. Set the "Subnet mask" (255.255.255.128)
            3. Set the "Gateway address" (9.xxx.xxx.129)
            Be sure to remember or write down the values of the "IP address" and "Subnet mask" fields as they will be needed in step 2, subsection d, of Section VII
            4. Click the "Save" button and click "OK" or "Yes" to any windows that may pop up
        Do not restart the BladeCenter Management Module

b. Configure the ESM network settings
    i. Click on the “Management” link in the “I/O Module Tasks” section
    ii. Configure and save the “New Static IP Configuration” fields in the “Bay 1 (Ethernet SM)” section if they are not already correct as listed in the “Current IP Configuration” section
        1. Set the “IP address” (9.xxx.xxx.147)
        2. Set the “Subnet mask” (255.255.255.128)
        3. Set the “Gateway address (9.xxx.xxx.129)
        4. Click the “Save” button
c. Configure the Serial Over LAN settings
    i. Click on the “Serial Over LAN” link in the “Blade Tasks” section
    ii. Configure and save the following fields in the “Serial Over LAN Configuration” section
        1. Select the “Enabled” option of the “Serial Over LAN” field
        2. Enter the correct “SOL VLAN ID”

           IBM and Nortel ESM’s:

           If you have an IBM or Nortel ESM, the value MUST be 4095.

           Cisco ESM’s:

           If you have a Cisco ESM, the value CANNOT be 4095. It can be any value you choose from 3 - 1001. You must remember this value as it will be used later in this document when configuring the Cisco ESM.
        3. Enter the “BSMP IP address range” (10.1.1.100)
        4. Set the “Accumulate timeout” field to 25 (default is 5)
        5. Set the “Send threshold” field (default is 250) if it is not set
        6. Set the “Retry count” field (default is 3) if it is not set
        7. Set the “Retry interval” field to 2500 (default is 250)
        8. Click the “Save” button

        Do not attempt to enable or disable SOL on any of the 8839 Blade Server’s in the “Serial Over LAN Status” section

3. Restart the BladeCenter Management Module
    a. Click on the “Restart MM” link in the “MM Control” section
    b. Click the “Restart” button in the “Restart MM” section
    c. Click the “OK” button in the confirmation window
    d. Click the “Yes” button to close the current Web interface
    e. Wait about 30 seconds or so, start a new Web browser, and reconnect to the BladeCenter Management Module Web interface

The BladeCenter Management Module is now enabled for SOL.

V. 8839 Blade Server BMC

Follow the directions outlined below to update the 8839 Blade Server BMC (Baseboard Management Controller). There is no configuration required for the 8839 Blade Server BMC to enable SOL.

Notes:

The 8839 Blade Server BMC code must be updated before attempting to update the 8839 Blade Server BIOS code.

The 8839 Blade Server SDR code will also be updated during the BMC flashing process.

1. Flash the 8839 Blade Server BMC
    a. Obtain the latest 8839 Blade Server BMC diskette image
    b. Create a diskette from the image obtained above
    c. Boot the diskette created above
    d. At the prompt, type “LCREFLSH.BAT” and press enter
        Note: This will take a long time to complete. Do not power off or reboot the 8839 Blade Server during this process. You must wait for it to complete. You will see status updates as the 8839 Blade Server is being updated.
    e. Reboot the 8839 Blade Server when the flashing operation has completed and proceed to the next section

The 8839 Blade Server BMC is now enabled for SOL.

VI. 8839 Blade Server BIOS

Note: The 8839 Blade Server BMC code must be updated (refer to Section V) before updating the 8839 Blade Server BIOS.

Follow the directions outlined below to update and configure the 8839 Blade Server BIOS to enable SOL.

1. Flash the 8839 Blade Server BIOS
    a. Obtain the latest 8839 Blade Server BIOS diskette images
    b. Create diskettes from the images obtained above
    c. Boot the first diskette created above
    d. Select option "1 – Update POST/BIOS" and press enter
    e. Enter "SBX44005.001" at the "Enter file name:" prompt
    f. Select the appropriate answers for all of the prompts until the flashing starts
    g. When prompted to "Press any key when this file "SBX44005.002" is in drive", insert the second diskette into the floppy drive and press enter
    h. Press the "Enter" key to confirm the message box that states "Request completed successfully"
    i. Remove the diskette from the drive
    j. Ensure the "YES" selection is highlighted and press the "Enter" key to reboot the system
2. Configure the 8839 Blade Server BIOS settings
    a. Press F1 as the 8839 Blade Server is booting to enter the setup utility
    b. Enter the "Devices and I/O Ports" selection
        i. Set the "Serial Ports" option to "Enabled"
        ii. Enter the "Remote Console Redirection" selection
            1. Set "BIOS Redirection Port" option to "Serial 2"
            Note: Newer BIOS revisions have the "BIOS Redirection Port" fixed to "Serial 2". Therefore, they no longer have this option.
            2. Set "Baud Rate" option to "19.2K"
            3. Set "Flow Control" option to "CTS/RTS"
            4. Set "Terminal Type" option to "VT100+"
    c. Press the "F10" key
    d. Ensure that the "OK" is highlighted and press enter to save the changes

Note: It is recommended that you remove and reinsert the 8839 Blade Server once you have updated the BCM, and BIOS.

The 8839 Blade Server BIOS is now enabled for SOL.

VII. IBM 4-Port Gigabit ESM (Ethernet Switch Module)

The following assumptions have been made for these directions

1. You are already connected to the BladeCenter Management Module Web Interface

Note: You will not be able to perform the directions outlined below if you used values for the network configuration of the IBM ESM that are not within the same subnet as the BladeCenter Management Module network interfaces (eth0 and eth1). Refer to Section IV for additional information.

Follow the directions outlined below to update the firmware of the IBM ESM. There is no configuration required for the IBM ESM to enable SOL.

1. Connect to the IBM ESM Web interface
   a. Click on the "Management" link under the "I/O Module Tasks" section

      Ensure that the "Current IP Configuration" section contains values that are within the same subnet as the BladeCenter Management Module network interfaces (eth0 and eth1) as this will be required in order to access the Web interface of the IBM ESM. If they are not, you MUST modify them before proceeding. Refer to Section IV for additional information.

   b. Click on the "Advanced Management" link under the "Bay 1 (Ethernet SM)*"
   c. Scroll down to the bottom of the page and click the "Start Web Session" button in the "Start Telnet/Web Session" section
      This will launch a new Web browser and connect to the IBM ESM Web interface
   d. Log in to the IBM ESM (the default User name is "USERID" and the default Password is "PASSW0RD")
2. Update the IBM ESM firmware
   a. Obtain the latest IBM ESM firmware file
   b. Click on the "Maintenance" link
   c. Click on the "Using Browser" link
   d. Click on the "Upgrade Firmware/Configuration" link
   e. Click the "Browse" button and select the file obtained in step "1a" above
   f. Click the "Start" button, answer "Yes" to any questions and wait for the firmware to be updated
   g. Close the Web browser
3. Restart the IBM ESM
   a. From the Management Module Web Interface, click on the "Power/Restart" link under the "I/O Module Tasks" section
   b. Check the box next to your IBM ESM and click on the "Restart Module(s) and Run Standard Diagnostics" link
   c. Click the "OK" button on the confirmation screen

The IBM ESM (Ethernet Switch Module) is now enabled for SOL.

VIII. Nortel Networks 4-Port Layer 2-7 and 6-Port Layer 2-3 Gigabit ESM (Ethernet Switch Module)

The following assumptions have been made for these directions

1. You are already connected to the BladeCenter Management Module Web Interface

Notes:

You will not be able to perform the directions outlined below if you used values for the network configuration of the Nortel ESM that are not within the same subnet as the BladeCenter Management Module network interfaces (eth0 and eth1). Refer to Section IV for additional information.

These directions require the presence of an accessible TFTP (Tiny FTP) server on your production network. Due to legal concerns, IBM can neither provide nor suggest any TFTP software products.

The latest firmware version should always be obtained from the IBM web site.

Follow the directions outlined below to update the firmware of the Nortel ESM. There is no configuration required for the Nortel ESM to enable SOL.

1. Update the Nortel ESM firmware
    a. Obtain the latest Nortel ESM firmware zip file
    b. Unzip the file obtained above into a temporary directory
    c. Copy the two image files, GbESM-AOS-xx.x.x.xx-os.img and GbESM-AOS-xx.x.x.xx -boot.img, from the temporary directory to the root of the TFTP server
    Where xx.x.x.xx is the current firmware version
    d. Connect to the Nortel ESM telnet interface
        i. Click on the “Management” link under the “I/O Module Tasks” section

        Ensure that the “Current IP Configuration” section contains values that are within the same subnet as the BladeCenter Management Module network interfaces (eth0 and eth1) as this will be required in order to access the telnet interface of the Nortel ESM. If they are not, you MUST modify them before proceeding. Refer to Section IV for additional information.

        ii. Click on the “Advanced Management” link under the “Bay 1 (Ethernet SM)*”
        iii. Scroll down to the bottom of the page and click the “Start Telnet Session” button in the “Start Telnet/Web Session” section
        This will launch a java telnet application and connect to the Nortel ESM
        iv. Log in to the Nortel ESM (the default Password is “admin”)
        v. When prompted to run “Setup Up” to configure the Nortel ESM, type “n” and press enter

e. Update the Nortel ESM OS image

Note: There are two OS images (image1 and image2) that reside in the Nortel ESM. Normally, the Nortel ESM will boot image1. However, you must determine which OS image is being used before updating the Nortel ESM firmware.

i. Type "/boot/cur" at the telnet prompt to determine which OS image is being used. The output from the "/boot/cur" command will state the name of the image (image1 or image2) that is currently being used. The text will be something like "Currently set to boot software image1".

Note: You MUST use image2 for the command in the next step if the output from the /boot/cur command states that image2 is currently empty

ii. Type "/boot/gtimg *imageX TFTPAddr* GbESM-AOS-xx.x.x.xx-os.img", where xx.x.x.xx is the current firmware version, at the telnet prompt and press enter
Where *imageX* is the name of the OS image (image1 or image2) that was determined in previous step, *TFTPAddr* is the IP address of the TFTP server on your production network where the image files reside, and xx.x.x.xx is the current firmware version

iii. Type "y" and press enter when prompted to "Confirm download operation"

iv. Wait for the flashing operation to complete

Note: Type "y" and press enter to boot from the new image if you were forced to update image2 because it was previously empty.

v. Type "exit" and press enter to terminate the Nortel ESM telnet interface

vi. Close the window in which the Nortel ESM telnet session was running

f. Restart the Nortel ESM

i. From the Management Module Web Interface, click on the "Power/Restart" link under the "I/O Module Tasks" section

ii. Check the box next to your Nortel ESM and click on the "Power Off Module(s)" link

iii. Click the "OK" button on the confirmation screen

iv. Check the box next to your Nortel ESM and click on the "Power On Module(s)" link

v. Click the "OK" button on the confirmation screen

Note: You must wait approximately 60 seconds for the Nortel ESM to fully restart before continuing

g. Reconnect to the Nortel ESM telnet interface by repeating step "d" above

h. Update the Nortel ESM boot image

i. Type "/boot/gtimg boot *TFTPAddr* GbESM-AOS-xx.x.x.xx-boot.img" at the telnet prompt and press enter

Where *TFTPAddr* is the IP address of the TFTP server on your production network where the image files reside and xx.x.x.xx is the current firmware version

i. Type “y” and press enter when prompted to “Confirm download operation”
j. Wait for the flashing operation to complete
k. Type “exit” and press enter to close the Nortel ESM telnet interface
l. Close the window in which the Nortel ESM telnet session was running
m. Restart the Nortel ESM by repeating step “f” above

The Nortel Networks 4-Port Layer 2-7 or 6-Port Layer 2-3 ESM (Ethernet Switch Module) is now enabled for SOL.

IX. Cisco Systems Intelligent Gigabit ESM (Ethernet Switch Module)

The following assumptions have been made for these directions

1. You are already connected to the BladeCenter Management Module Web Interface

Notes:

You will not be able to perform the directions outlined below if you used values for the network configuration of the Cisco ESM that are not within the same subnet as the BladeCenter Management Module network interfaces (eth0 and eth1). Refer to Section IV for additional information.

VLAN ID 3 will be used for demonstration purposes. You must use the value you assigned to the "SOL VLAN ID" of the BladeCenter Management Module in step 2, c, ii, 2 of Section IV.

These directions include removing the SOL VLAN ID from the external ports of the Cisco ESM. You must complete these steps. There could be a security risk if you do not.

The internal interfaces of the Cisco ESM must be set to trunk mode not access mode in order for SOL to function. Trunk mode is the default configuration however the instructions for configuring the mode are included below and should be performed to ensure that the configuration is correct.

Follow the directions outlined below to configure the Cisco ESM to enable SOL.

1. Configure the Cisco ESM
    a. Connect to the Cisco ESM telnet interface
        i. Click on the "Management" link under the "I/O Module Tasks" section

        Ensure that the "Current IP Configuration" section contains values that are within the same subnet as the BladeCenter Management Module network interfaces (eth0 and eth1) as this will be required in order to access the telnet interface of the Cisco ESM. If they are not, you MUST modify them before proceeding. Refer to Section IV for additional information.

        ii. Click on the "Advanced Management" link under the "Bay 1 (Ethernet SM)*"
        iii. Scroll down to the bottom of the page and click the "Start Telnet Session" button in the "Start Telnet/Web Session" section
        This will launch a java telnet application and connect to the Cisco ESM
        iv. Log in to the Cisco ESM (the default User Name is "USERID" and the default Password is "PASSW0RD")

b. Activate the SOL VLAN ID of the Cisco ESM
    i. Type “en” and press Enter
    ii. Type “config t” at the prompt and press Enter
    iii. Type “vlan 3” and press Enter
    iv. Type “state active” and press Enter
    v. Type “end” and press Enter
    vi. Type “wri” and press Enter to save the configuration
    Note: Do not exit the telnet interface at this time
c. Remove the SOL VLAN ID from the external ports of the Cisco ESM
    i. Type “config t” at the prompt and press Enter
    ii. Type “int range gi0/17 - 20” and press Enter
    iii. Type “switchport trunk allowed vlan remove 3” and press Enter
    iv. Type “end” and press Enter
    v. Type “wri” and press Enter to save the configuration
    Note: Do not exit the telnet interface at this time
d. Configure the internal interfaces for trunk mode and add the SOL VLAN ID
    i. Type “config t” at the prompt and press Enter
    ii. Type “int range gi0/1 - 14” and press Enter
    iii. Type “switchport mode trunk” and press Enter
    iv. Type “exit” and press Enter
    v. Type “int range gi0/1 - 16” and press Enter
    vi. Type “sw trunk allow vlan add 3” and press Enter
    vii. Type “end” and press Enter
    viii. Type “wri” and press Enter to save the configuration
e. Exit the Cisco ESM telnet session
    i. Type “exit” and press enter to terminate the Cisco ESM telnet interface
    ii. Close the window in which the Cisco ESM telnet session was running

The Cisco Systems Intelligent Gigabit ESM (Ethernet Switch Module) is now enabled for SOL.

X. Completing the Configuration

The following assumptions have been made for these directions

1. You are already connected to the BladeCenter Management Module Web Interface

Now that all of the required items have been updated and configured, follow the directions outlined below to complete the configuration.

1. Enable SOL on the 8839 Blade Server(s)
    a. Click on the “Serial Over LAN” link in the “Blade Tasks” section
    b. Check the boxes next to the 8839 Blade Server(s) that you wish to enable SOL on in the “Serial Over LAN Status” section
    c. Click on the “Enable Serial Over LAN” link at the bottom
    d. After the page reloads, the “SOL” section on the table should say “Enabled” for the 8839 Blade Server(s) you selected
    e. The “SOL Session” section of the table should say “Not Ready” for the 8839 Blade Server(s) you selected
2. Power Up or Restart the 8839 Blade Server(s)
    a. Click on the “Power/Restart” link in the “Blade Tasks” section
    b. Check the 8839 Blade Server(s) that you have enabled SOL on and click on either the “Power On Blade” or “Restart Blade” depending on the current status of your 8839 Blade Server(s)
    c. Click the “OK” button on the confirmation window
    d. Click the “OK” button on the information window and wait for the Web page to refresh
3. Check the status of the 8839 Blade Server(s)
    a. Click on the “Serial Over LAN” link in the “Blade Tasks” section
    b. Scroll down and ensure that the “SOL Session” section of the table in the “Serial Over LAN Status” for the selected 8839 Blade Server(s) now says “Ready”

The SOL configuration is now complete.

XI. Enabling SOL Sessions for Red Hat Enterprise Linux ES 2.1

The following assumptions have been made for these directions

1. You are logged in as the "root" user

Follow the directions outlined below to enable SOL sessions for the Red Hat Enterprise Linux ES 2.1 Operating System.

Note that a default installation of Red Hat Enterprise Linux ES 2.1 was used while developing this document. The file names, structures, and commands described in this document may differ from other versions of Red Hat Linux.

Note: Hardware Flow Control is used to prevent character loss over serial connections due to heavy amounts of data. Hardware Flow Control for Linux operating systems is required for SOL to function properly.

You must reboot the Red Hat Enterprise Linux ES 2.1 Operating System after completing these directions to enable SOL.

General Configuration:

1. Modify the /etc/inittab file
   a. Add the following line to the end of the "# Run gettys in standard runlevels" section of the /etc/inittab file to enable users to log in at the SOL console
      i. 7:2345:respawn:/sbin/agetty –h ttyS1 19200 vt102
2. Modify the /etc/securetty file
   a. Add the following line at the bottom of the /etc/securetty file to enable users to log in as "root" at the SOL console
      i. ttyS1

LILO Configuration:

Follow the directions outlined below if you are using LILO.

1. Modify the /etc/lilo.conf file
   a. Append the following text to the first "default=…" line
      i. -Monitor
   b. Comment out the "map=…" line by adding a "#" in front of the word "map"
   c. Comment out the "message=…" line by adding a "#" in front of the word "message"
   d. Add the following line before the first "image=…" line
      i. # This will allow you to only Monitor the OS boot via SOL
   e. Append the following text to the first "label=…" line
      i. -Monitor
   f. Add the following line to the first "image= " section to enable SOL
      i. append="console=ttyS1,19200n8 console=tty1"
   g. Add the following lines between the two "image…" sections
      i. # This will allow you to Interact with the OS boot via SOL
      ii. image=/boot/vmlinuz-2.4.9-e.12smp
      iii. label=linux-Interact
      iv. initrd=/boot/initrd-2.4.9-e.12smp.img
      v. read-only
      vi. root=/dev/hda6
      vii. append="console=tty1 console=ttyS1,19200n8 "

Original /etc/lilo.conf contents

```
prompt
timeout=50
default=linux
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear

image=/boot/vmlinuz-2.4.9-e.12smp
        label=linux
        initrd=/boot/initrd-2.4.9-e.12smp.img
        read-only
        root=/dev/hda6

image=/boot/vmlinuz-2.4.9-e.12
        label=linux-up
        initrd=/boot/initrd-2.4.9-e.12.img
        read-only
        root=/dev/hda6
```

Modified /etc/lilo.conf contents

```
prompt
timeout=50
default=linux-Monitor
boot=/dev/hda
#map=/boot/map
install=/boot/boot.b
#message=/boot/message
linear

# This will allow you to only Monitor the OS boot via SOL
image=/boot/vmlinuz-2.4.9-e.12smp
        label=linux-Monitor
        initrd=/boot/initrd-2.4.9-e.12smp.img
        read-only
        root=/dev/hda6
        append="console=ttyS1,19200n8 console=tty1"

# This will allow you to Interact with the OS boot via SOL
image=/boot/vmlinuz-2.4.9-e.12smp
        label=linux-Interact
        initrd=/boot/initrd-2.4.9-e.12smp.img
        read-only
        root=/dev/hda6
        append="console=tty1 console=ttyS1,19200n8"

image=/boot/vmlinuz-2.4.9-e.12
        label=linux-up
        initrd=/boot/initrd-2.4.9-e.12.img
        read-only
        root=/dev/hda6
```

2. Type “lilo” and press enter to store and activate the new LILO configuration
   Note: When the operating system starts to boot, you will now see a “LILO boot:” prompt instead of the usual GUI interface. Pressing the “Tab” key while at this prompt will result in all of the boot options being listed. To load the operating system in Interactive mode, you would type “linux-Interact” and press enter.

GRUB Configuration:

Follow the directions outlined below if you are using GRUB.

1. Modify the /boot/grub/grub.conf file
   a. Comment out the "splashimage=…" line by adding a "#" in front of the word "splashimage"
   b. Add the following line before the first "title=…" line
      i. # This will allow you to only Monitor the OS boot via SOL
   c. Append the following text to the first "title=…" line
      i. SOL Monitor
   d. Append the following text to the "kernel/…" line of the first "title…" section
      i. console=ttyS1,19200 console=tty1
   e. Add the following lines between the two "title…" sections
      i. # This will allow you to Interact with the OS boot via SOL
      ii. title Red Hat Linux (2.4.9-e.12smp) SOL Interactive
      iii. root (hd0,0)
      iv. kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6 console=tty1 console=ttyS1,19200
      v. initrd /initrd-2.4.9-e.12smp.img

Original /boot/grub/grub.conf contents

```
#grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#               all kernel and initrd paths are relative to /boot/, eg.
#               root (hd0,0)
#               kernel /vmlinuz-version ro root=/dev/hda6
#               initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Enterprise Linux ES (2.4.9-e.12smp)
        root (hd0,0)
        kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6
        initrd /initrd-2.4.9-e.12smp.img
title Red Hat Enterprise Linux ES-up (2.4.9-e.12)
        root (hd0,0)
        kernel /vmlinuz-2.4.9-e.12 ro root=/dev/hda6
        initrd /initrd-2.4.9-e.12.img
```

Modified /boot/grub/grub.conf contents

```
#grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#               all kernel and initrd paths are relative to /boot/, eg.
#               root (hd0,0)
#               kernel /vmlinuz-version ro root=/dev/hda6
#               initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
# This will allow you to only Monitor the OS boot via SOL
title Red Hat Enterprise Linux ES (2.4.9-e.12smp) SOL Monitor
   root (hd0,0)
#Note:  The following "kernel…" line is all one line, not two separate lines
#       The text has wrapped in this example
   kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6 console=ttyS1,19200
console=tty1
   initrd /initrd-2.4.9-e.12smp.img
# This will allow you to Interact with the OS boot via SOL
title Red Hat Linux (2.4.9-e.12smp) SOL Interactive
   root (hd0,0)
#Note:  The following "kernel…" line is all one line, not two separate lines
#       The text has wrapped in this example
   kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6 console=tty1
console=ttyS1,19200
   initrd /initrd-2.4.9-e.12smp.img
title Red Hat Enterprise Linux ES-up (2.4.9-e.12)
   root (hd0,0)
   kernel /vmlinuz-2.4.9-e.12 ro root=/dev/hda6
   initrd /initrd-2.4.9-e.12.img
```

Red Hat Enterprise Linux ES 2.1 configuration is now complete. Do not forget to reboot the operating system for the changes to take effect.

XII. Enabling SOL Sessions for SUSE SLES 8.0

The following assumptions have been made for these directions

1. You are logged in as the "root" user

Note that a default installation of SUSE SLES 8.0 was used while developing this document. The file names, structures, and commands described in this document may differ from other versions of SUSE Linux.

Note: Hardware Flow Control is used to prevent character loss over serial connections due to heavy amounts of data. Hardware Flow Control for Linux operating systems is required for SOL to function properly.

You must reboot the SUSE SLES 8.0 Operating System after completing these directions to enable SOL.

Follow the directions outlined below to enable SOL sessions for the SUSE SLES 8.0 Operating System.

1. Modify the /etc/inittab file
   a. Add the following line to the end of the "# getty-programs for the normal runlevels" section of the /etc/inittab file to enable users to log in at the SOL console
      i. 7:2345:respawn:/sbin/agetty –h ttyS1 19200 vt102
2. Modify the /etc/securetty file
   a. Add the following line after the "tty6" line in the /etc/securetty file to enable users to log in as "root" at the SOL console
      i. ttyS1
3. Modify the /boot/grub/menu.lst file
   a. Comment out the "gfxmenu…" line by adding a "#" in front of the word "gfxmenu"
   b. Add the following line before the first "title…" line
      i. # This will allow you to only Monitor the OS boot via SOL
   c. Append the following text to the first "title…" line
      i. SOL Monitor
   d. Append the following text to the "kernel…" line of the first "title…" section
      i. console=ttyS1,19200 console=tty1
   e. Add the following lines between the first two "title…" sections
      i. # This will allow you to Interact with the OS boot via SOL
      ii. title linux SOL Interactive
      iii. kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot vga=791 console=tty1 console=ttyS1,19200
      iv. initrd (hd0,1)/boot/initrd

   Note: See next page for an example of a modified /boot/grub/menu.lst file.

Original /boot/grub/menu.lst contents

```
gfxmenu (hd0,1)/boot/message
color white/blue black/light-gray
default 0
timeout 8

title linux
   kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot   vga=791
   initrd (hd0,1)/boot/initrd
title floppy
   root
    chainloader +1
title failsafe
   kernel (hd0,1)/boot/vmlinuz.shipped root=/dev/hda2 ide=nodma apm=off
vga=normal nosmp disableapic maxcpus=0 3
   initrd (hd0,1)/boot/initrd.shipped
```

Modified /boot/grub/menu.lst contents

```
#gfxmenu (hd0,1)/boot/message
color white/blue black/light-gray
default 0
timeout 8

# This will allow you to only Monitor the OS boot via SOL
title linux SOL Monitor
#Note:  The following "kernel..." line is all one line, not two separate lines
#          The text has wrapped in this example
   kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot   vga=791
console=ttyS1,19200 console=tty1
   initrd (hd0,1)/boot/initrd
# This will allow you to Interact with the OS boot via SOL
title linux SOL Interactive
#Note:  The following "kernel..." line is all one line, not two separate lines
#          The text has wrapped in this example
   kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot   vga=791
console=tty1 console=ttyS1,19200
   initrd (hd0,1)/boot/initrd
title floppy
   root
    chainloader +1
title failsafe
   kernel (hd0,1)/boot/vmlinuz.shipped root=/dev/hda2 ide=nodma apm=off
vga=normal nosmp disableapic maxcpus=0 3
   initrd (hd0,1)/boot/initrd.shipped
```

SUSE SLES 8.0 configuration is now complete. Do not forget to reboot the operating system for the changes to take effect.

XIII. Installing the 8839 Blade Server Intel Ethernet Controller Device Driver for Linux Operating Systems

The following assumptions have been made for these directions

1. You are logged in as the "root" user
2. The development tools packages have already been installed
3. The kernel source package has already been installed

Follow the directions outlined below to install the 8839 Blade Server Intel Ethernet Controller device driver.

Note that default installations of Red Hat Enterprise Linux ES 2.1 and SUSE SLES 8.0 were used while developing this document. The file names, structures, and commands described in this document may differ from other versions of Linux operating systems.

The latest device driver version should always be obtained from the IBM web site. The version listed in these instructions is for example purposes only.

The kernel source and development tools packages must be installed before attempting to use the directions outlined below.

1. Obtain the latest version of 8839 Blade Server Intel Ethernet Controller device driver source package
2. Mount the media containing the 8839 Blade Server Intel Ethernet Controller device driver source obtained above
    a. If the media is a CD
        i. Red Hat Enterprise Linux ES 2.1
            1. Ensure the /mnt/cdrom directory exists, type "mkdir /mnt/cdrom" and press enter if it does not
            2. Type "mount /dev/scd0 –t iso9660 –o ro /mnt/cdrom" and press enter
        ii. SUSE SLES 8.0
            1. Ensure the /media/cdrom directory exists, type "mkdir /media/cdrom" and press enter if it does not
            2. Type "mount /dev/scd0 –t iso9660 –o ro /media/cdrom" and press enter
    b. If the media is a diskette
        i. Red Hat Enterprise Linux ES 2.1
            1. Ensure the /mnt/floppy directory exists, type "mkdir /mnt/floppy" and press enter if it does not
            2. Type "mount /dev/sda –o auto /mnt/floppy" and press enter
        ii. SUSE SLES 8.0
            1. Ensure the /media/floppy directory exists, type "mkdir /media/floppy" and press enter if it does not
            2. Type "mount /dev/sda –o auto /media/floppy" and press enter

3. Compile and install the 8839 Blade Server Intel Ethernet Controller device driver
   Note: The temporary directory "/usr/local/src/e1000" will be used for the instructions in this step.
   a. Create the temporary directory if it does not already exist
      i. Type "mkdir /usr/local/src/e1000" and press enter
   b. Change to the temporary directory
      i. Type "cd /usr/local/src/e1000" and press enter
   c. Copy the 8839 Blade Server Intel Ethernet Controller device driver source file from the media to the temporary directory
      i. Type "cp {source directory}/e1000-5.2.22.1.tar.gz ." and press enter
   d. Untar the source package
      i. Type "tar zxf e1000-5.2.22.1.tar.gz" and press enter
   e. Change to the source directory
      i. Type "cd e1000-5.2.22.1/src" and press enter
   f. Compile the device driver
      i. Type "make install" and press enter
   g. Install the device driver
      i. Type "insmod e1000" and press enter
4. Unmount the media containing the 8839 Blade Server Intel Ethernet Controller device driver source
   a. Type "cd" and press enter
   b. If the media is a CD
      i. Red Hat Enterprise Linux ES 2.1
         1. Type "umount /mnt/cdrom" and press enter
      ii. SUSE SLES 8.0
         1. Type "umount /media/cdrom" and press enter
   c. If the media is a diskette
      i. Red Hat Enterprise Linux ES 2.1
         1. Type "umount /mnt/floppy" and press enter
      ii. SUSE SLES 8.0
         1. Type "umount /media/floppy" and press enter
5. Configure the network interfaces for the Red Hat Enterprise Linux ES 2.1 or SUSE SLES 8.0 operating system
   Configuring the network interfaces and settings of the Red Hat Enterprise Linux ES 2.1 and SUSE SLES 8.0 operating systems is beyond the scope of this document. Please refer to the documentation provided with your operating system for these instructions.

The installation of the 8839 Blade Server Intel Ethernet Controller device driver is complete.

XIV. Enabling SOL Sessions for Windows 2003 Standard Edition

The following assumptions have been made for these directions

1. You are logged in as a user that has administrative access

Note that a default installation of Windows 2003 Standard Edition was used while developing this document.

Note that in some installations, you may have to remove or uninstall the COM2 device from the Windows device manager in order for SOL to function. Uninstalling the COM2 device is beyond the scope of this document. Please refer to the documentation for your operating system.

You must reboot the Windows 2003 Standard Edition Operating System after completing these directions to enable SOL.

Follow the directions outlined below to enable SOL sessions for the Windows 2003 Standard Edition Operating System.

1. Determine which boot entry ID to modify
   a. From a Windows command prompt, type "bootcfg" and press enter
      This will display the current boot options
   b. Locate the line in the "Boot Entries" section that says "OS Friendly Name: Windows Server 2003, Standard"
   c. Directly above that line will be the boot entry ID
      For example: "Boot entry ID: 1"
   d. Note this boot entry ID as it will be used in the next step
2. Enable EMS
   a. From a Windows command prompt, type "bootcfg /EMS ON /PORT COM2 /BAUD 19200 /ID {x}", where {x} is the boot entry ID as determined in step 1 above, and press enter
3. Verify that EMS is enabled
   a. From a Windows command prompt, type "bootcfg" and press enter
      This will display the current boot options
   b. Verify that the following modifications exist
      i. The following should be in the "Boot Loader Settings" section
         1. "redirect: COM2"
         2. "redirectbaudrate: 19200"
      ii. The "OS Load Options:" line in the "Boot Entries" section should have "/redirect" appended

Original bootcfg program output

```
Boot Loader Settings
--------------------
timeout:                30
default:                multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

Boot Entries
------------
Boot entry ID:          1
OS Friendly Name:       Windows Server 2003, Standard
Path:                   multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
OS Load Options:        /fastdetect
```

Modified bootcfg program output

```
Boot Loader Settings
--------------------
timeout:                30
default:                multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
redirect:               COM2
redirectbaudrate:       19200

Boot Entries
------------
Boot entry ID:          1
OS Friendly Name:       Windows Server 2003, Standard
Path:                   multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
OS Load Options:        /fastdetect /redirect
```

The Windows 2003 Standard Edition Operating System configuration is now complete. Do not forget to reboot the operating system for the changes to take effect.

XV. Using SOL

This section describes how to start and stop BladeCenter Management Module telnet CLI and SOL sessions as well as other special key sequences you can use while in an SOL session.

Starting BladeCenter Management Module Telnet CLI Sessions:

1. From any command prompt, type "telnet {location}", where location is the hostname or IP address of the BladeCenter Management Module
2. Log in to the BladeCenter Management Module (the default user name is USERID and the default password is PASSW0RD)

Starting SOL Sessions:

1. Type "console –T system:blade[x]" from a BladeCenter Management Module telnet CLI prompt, where blade[x] (note that the brackets "[ ]" are required) is the number of the 8839 Blade Server (1 -14 in the chassis) that you wish to start the SOL session with.

Note: The BladeCenter Management Module automatically stores the previous 8 KB (Kilobytes) of serial data that was transmitted by each 8839 Blade Server even when SOL sessions are not active. When an SOL session is established, all of the previous serial data, up to 8 KB, is automatically displayed. If there is no previous data available when the SOL session is started, the cursor will remain on the command line until new serial data is transmitted.

Rebooting 8839 Blade Server(s) via SOL sessions:

You no longer have to exit the current SOL and use the telnet CLI of the BladeCenter Management Module to reboot the 8839 Blade Server. Instead, you can type the following sequence of commands from within the SOL session.

1. Key sequence ("Esc" → "R" → "Esc" → "r" → "Esc" → "R")
    a. Press the escape ("Esc") key
    b. Type a capital "R" by pressing the "Shift" and "r" keys at the same time
    c. Press the escape ("Esc") key again
    d. Type a lowercase "r"
    e. Press the escape ("Esc") key again
    f. Type a capital "R" by pressing the "Shift" and "r" keys at the same time

Exiting SOL Sessions:

1. Key sequence ("Esc" → "(")
    a. Press the escape ("Esc") key
    b. Type a "(" by pressing the "Shift" and the "9" key at the same time

Note: Exiting an SOL session does not stop the flow of serial data

Exiting BladeCenter Management Module Telnet CLI Sessions:

1. Type "exit" at the BladeCenter Management Module telnet CLI prompt after exiting an SOL session

XVI. Installing and Configuring SSH (Secure Shell Server) for SOL

The following assumptions have been made for these directions

1. You are already connected to the BladeCenter Management Module Web Interface
2. You can connect to the external IBM web site

Follow the directions outlined below to install and configure SSH for SOL. You can omit step 1 if you have previously installed the SSL/SSH security key file.

1. Obtain and install the SSL and SSH security file from IBM
    a. Click on the “Security” link under the “MM Control” section
    b. Obtain the latest SSL/SSH security key file from IBM by clicking on the “BladeCenter firmware update” link in the “Install SSL/SSH” section and following the directions
    c. Click the “Browse…” button and select the file you downloaded in the previous instruction
    d. Click the “Install SSL/SSH” button
    e. Click on the “configure and enable” link in the “Install SSL/SSH” section
2. Generate the SSH Server Private Key
    a. Click the “Generate SSH Server Private Key” button in the “SSH Server Key Management” section
    b. Click the “OK” button in the confirmation window and wait for the process to complete
3. Enable SHH
    a. Set the “SSH Server” option in the “Secure Shell (SSH) Server” section to “Enabled” and press the “Save” button
    b. Click the “OK” button in the confirmation window
4. Restart the Management Module
    a. Click on the “Restart MM” link in the “MM Control” section
    b. Click the “Restart” button in the “Restart MM” section
    c. Click the “OK” button in the confirmation window

The installation and configuration of SSH is complete, you can now use your favorite SSH client to start secured telnet and SOL sessions to the Management Module and 8839 Blade Server(s).