Sun Fire™ B10n Content Load Balancing Blade Version 1.2 Update Product Notes

Sun Microsystems, Inc.
www.sun.com

Part No. 817-6211-10
March 2004, Revision A

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Please
Recycle

Adobe PostScript™

Declaration of Conformity

Compliance Model Number:	BP-4
Product Family Name:	Sun Fire B10n Content Load Balancing Blade

EMC

USA—FCC Class A

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This equipment may not cause harmful interference.
2. This equipment must accept any interference that may cause undesired operation.

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

As Telecommunication Network Equipment (TNE) in Both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class A
EN61000-3-2	Pass
EN61000-3-3	Pass
EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz, and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor signal Lines > 10m
EN61000-4-6	3 V
EN61000-4-11	Pass

As Information Technology Equipment (ITE) Class A per (as applicable):

EN55022:1998/CISPR22:1997	Class A
EN55024:1998 Required Limits:	
EN61000-4-2	4 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m
EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines, 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
EN61000-4-6	3 V
EN61000-4-8	1 A/m
EN61000-4-11	Pass
EN61000-3-2:1995 + A1, A2, A14	Pass
EN61000-3-3:1995	Pass

Safety: This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN60950:2000, 3rd Edition	TÜV Rheinland Certificate No. xxxxxxxxxxxx		
IEC 60950:2000, 3rd Edition	CB Scheme Certificate No. xxxxxxxxxxxx		
Evaluated to all CB Countries			
UL 60950, 3rd Edition, CSA C22.2 No. 60950-00	File:	Vol.	Sec.
UL 60950, 3rd Edition, CSA C22.2 No. 950-00	File:	Vol.	Sec.
FDA DHHS Accession Number (Monitors Only)			

Supplementary Information: This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski DATE
Manager, Compliance Engineering
Sun Microsystems, Inc.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054 U.S.A.
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J. Dullaghan DATE
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395 Fax: +44 1 506 670 011

Contents

Sun Fire B10n Content Load Balancing Blade Version 1.2 Update Product Notes

This document contains important information about the Sun Fire™ B10n Content Load Balancing Blade Version 1.2 Update application software and the new server modules. This version includes all the features from Version 1.1, 1.2, and 1.2 Update. The application software is not changed with this release; only new server modules are provided.

Note – The current Sun Fire B10n content load balancing blades are shipped with the Version 1.1 software. This document explains how to upgrade your software to the latest version.

Note – This document describes all of the new features for the Sun Fire B10n Content Load Balancing Blade Version 1.2 Update release. The administration guide is not updated for this release.

Viewing the Latest Product Notes

Additional issues may arise after the publication of this version of the product notes. For the latest information, refer to the latest version of this document available at:

```
http://wwws.sun.com/products-n-solutions/hardware/docs/Servers/
Workgroup_Servers/Sun_Fire_Blade_Platform/Sun_Fire_b100s/
index.html
```

Software Release Features

New Features for This Release

Software release 1.2 Update provides support for the following hardware and software:

- Sun Fire B100s/V210/V240—Solaris 8 HW 02/04, Solaris 9 12/03
- Sun Fire B100x/B200x/V60/V65—Red Hat Linux Advanced Server (RHAS) 2.1 – Update 2 and RHAS 2.1, Enterprise Linux 3.0, SuSe Linux Enterprise Server (SLES) 8.0-SP3, Solaris 9 x86 12/03

Key Feature for 1.2 Update:

- External server load balancing

New Features Supported in Version 1.1.x

The Sun Fire B10n content load balancing blade application software release 1.1 adds high availability pair blade failover and path failover as well as support for the Sun Fire B10p SSL proxy blade.

New Features Supported in Version 1.2 Update

The rule build performance has been improved. The performance increase is up to five times faster than previous versions.

Supports no VLAN mode for Red Hat Enterprise Linux AS 2.1.

Software release 1.2 Update includes support for the following operating systems listed in TABLE 1.

TABLE 1 Supported Servers and Operating Systems

Operating System	Version	SPARC/x86	SF B1600 Server Blades			External Server		VLANs
			SF B100s	SF B100x	SF B200x	SF V60/65x	SF V210/240	
Solaris	8 HW 12/02	SPARC	X				X	Yes
Solaris	8 HW 5/03	SPARC	X				X	Yes
Solaris	8 HW 7/03	SPARC	X				X	Yes
Solaris	8 HW 2/04	SPARC	X				X	Yes
Solaris	9 8/03	SPARC	X				X	Yes
Solaris	9 12/03	SPARC	X				X	Yes
Red Hat Enterprise Linux	AS 2.1	x86		X	X			No
Red Hat Enterprise Linux	AS 2.1 Update-2	x86		X	X	X		No
Red Hat Enterprise Linux	EL 3.0	x86		X	X	X		Yes
SuSe	SLES 8.0 SP-3	x86		X	X			Yes
x86 Solaris	9 8/03	x86				X		No
x86 Solaris	9 12/03	x86		X	X	X		No

Zip files are available at the Sun Download Center at the following URL:
`http://wwws.sun.com/software/download/network.html`

Enter **`B10n`** and select Search the Download Center. Select Sun Fire B10n Content Load Balancing. Zip files listed in TABLE 2 are available.

TABLE 2 Zip Files Available at the Sun Download Center

Software Components	Zip File Name
BSC firmware	`SunFire_B10n-`*version#*`-BSCFirmware.zip`
B10n application software	`SunFire_B10n-`*version#*`-Application.zip`

Blade server module	`SunFire_B10n-`*version#*`-SolarisModule.zip`
	`SunFire_B10n-`*version#*`-LinuxModule.zip`

Administration Guide and Product Notes	`SunFire_B10n-`*version#*`-Docs.zip`

The Role of the Content Load Balancing Blade

The Sun Fire B10n blade is a component within a larger system ultimately delivering highly available network services to a client population over an IP-based network. This section describes the role of such a highly integrated content load balancer within the larger system.

The minimal set of components comprising the system encompasses:

- One or more Sun Fire B1600 blade system chassis
- One or more Sun Fire B10n blades
- One or two Switch and System Controller (SSC) units per system chassis
- One or more servers. Servers can be any mix of blade servers housed in B1600 blade system chassis and stand-alone Sun servers external to the chassis but connected to the same Ethernet broadcast domain (Layer 2 network)

Additionally, the system may have:

- One or more SSL proxy blades
- External distribution switches and routers extending one or more of the networks
- Additional servers providing content, local name and configuration services, and aggregate management for one or multiple shelves. These servers may participate in the overall system by supporting various TFTP, NFS, DHCP, DNS, and N1 deployment related functions

In general terms, the intra-shelf network topology formed by connecting the Sun Fire B1600 system components is either a single or a dual redundant Layer 2 topology with blades “one-arm” connected to each of the switch fabrics. The switch fabric is VLAN partitionable for strict traffic isolation. SSC switches and uplinks can be used for a simple inter-shelf network, or connected to external distribution switches for larger configurations.

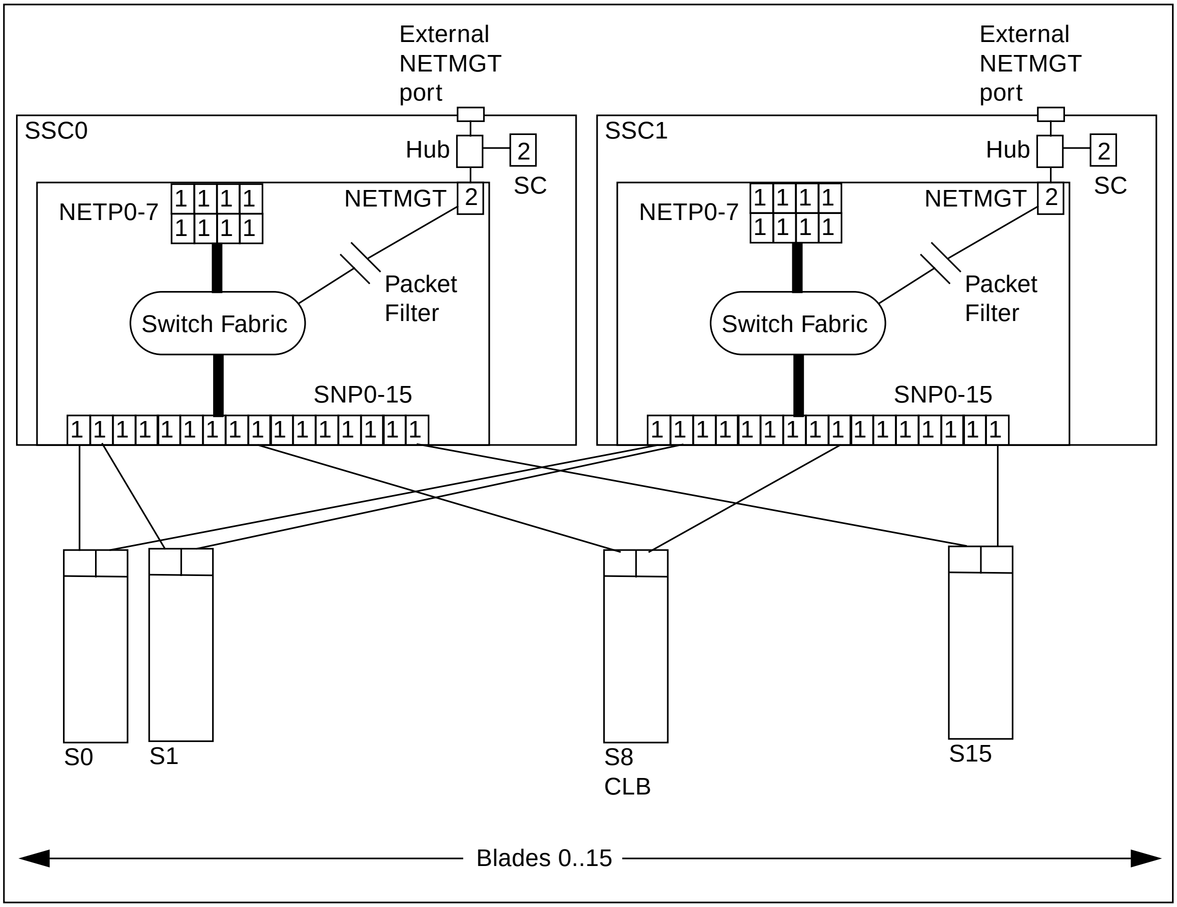

FIGURE 1 Ethernet Ports and Interfaces on the B1600 System Chassis and their Default VLAN Numbers

FIGURE 1 shows the intra-shelf network, where a Sun Fire B10n blade (shown in slot S8) can reside in any slot (S0 through S15) and connect to both SSC0 and SSC1 switch fabrics. The uplinks are labeled NETP0 through NETP7.

The numerals associated with each port (either 1 or 2), represent the VLAN numbers programmed into the system by default. The numbers indicate that there is one data VLAN (1), and one management VLAN (2). Further VLAN partitioning might be desirable as shown in FIGURE 2. The actual VLAN-ID assignment can be coordinated with the VLANs used in the external switches, or its scope can be limited to the internal switches, by keeping the uplinks as untagged VLANs.

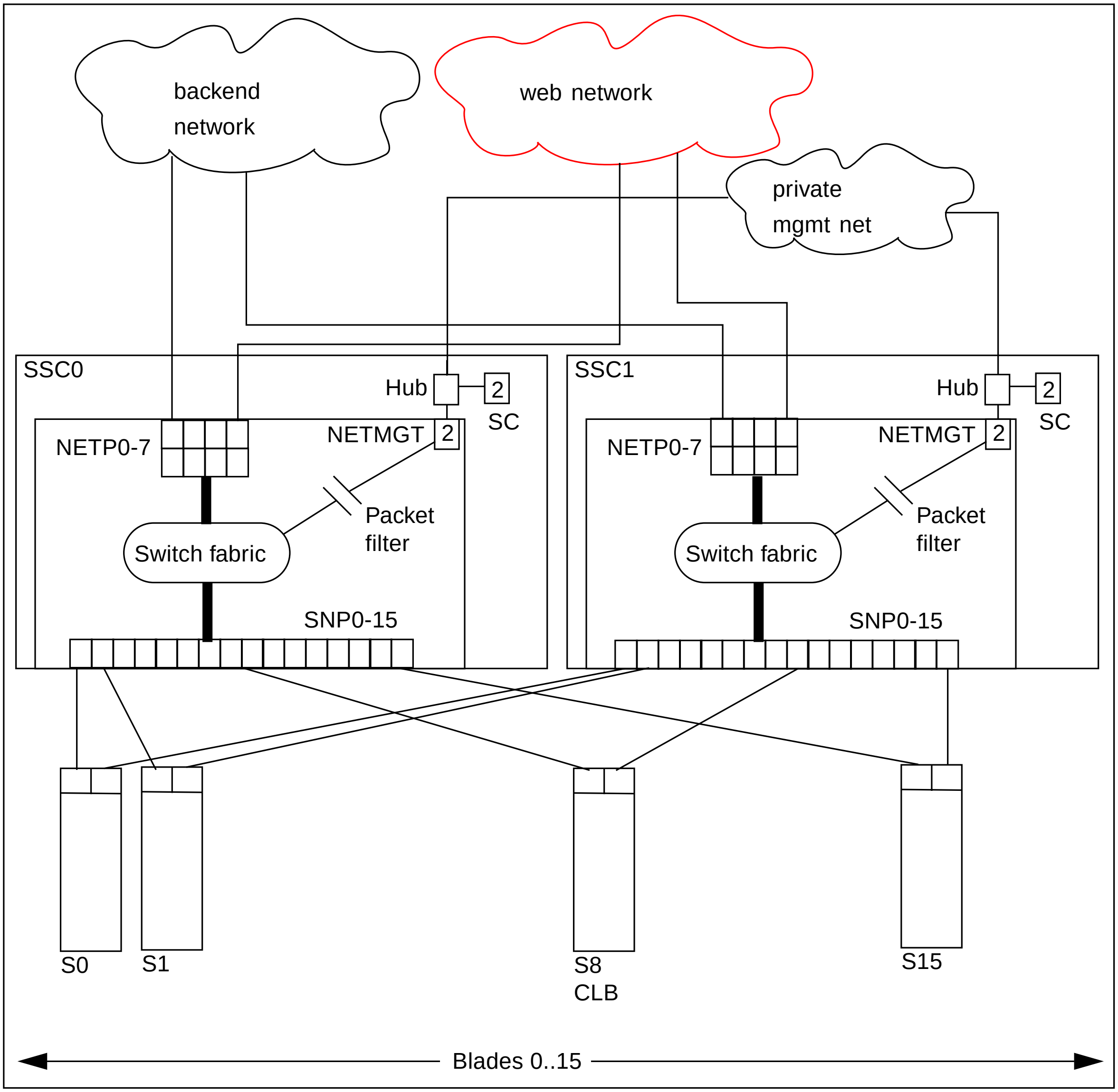

FIGURE 2 Dedicated Management Network and Web Server Network Isolated from the Backend Network

Load Balancing

The role of the content load balancer is to present a set of highly available network services. These services can be transported over http, TCP, or UDP, and are addressable through one or more Virtual IP addresses (VIPs), that the content load balancer is responsible for:

- Providing one level of address indirection so that the number and nature of actual servers can transparently evolve over time.
- Dividing requests among servers grouped in load balancing groups so that the total service demand can be satisfied through horizontal scaling.
- Maintaining persistence for clients or groups of clients requesting services that require affinity, that is, services where multiple consecutive requests must be satisfied by the same server.
- Delivering highly available services by taking responsibility for the failover functions that alter network paths, servers, and load balancer pairs upon service failure detection.
- Associating services to VLANs that partitions are based on meaningful criteria (service owner, back-end network, and the like).
- Participating one or more SSL proxy blades in the request packet flow whenever SSL encryption/decryption is necessary.
- Providing application monitoring through a user scripting interface.

VIPs are the routable IP addresses that clients obtain for the service though DNS lookups. A VIP address is *owned* by one content load balancer at a given time. VIPs are preserved through the content load balancer all the way to servers. Requests are directed to servers by rewriting their MAC addresses and their VLAN tags.

A service is identified by a 3-tuple comprising of the VIP, the Layer 4 protocol value (TCP or UDP), and TCP/UDP destination port. A multi-homed service can be associated with more than one 3-tuple. For example, two different VIPs can point to the same service. One of the initial steps in setting up the load balancer is to configure a service through the command line interface. Configurations can be input through the console interface by manual command line entry, scripted command sets or importing `config` files.

Load balancing or the server forwarding decision for a particular service is controlled by one or more rules. There are three basic types of rules, IP rules (layer 4), static HTTP and dynamic HTTP. An IP rule consists of source IP and source port, both have associated masks which enable subnets or port groups to be defined. Static HTTP (Layer 7) provides direct URL matching where as dynamic HTTP provides wild carding of various parameters. Rule matching is based on a priority match where priority is determined by rule type or assigned priority. If IP rule priority is Low, the order is HTTP static, HTTP dynamic, and IP rule. If IP rule priority is set to High, the order is IP rule, HTTP static and HTTP dynamic. The number of bits configured determines order within a rule type.

The next parameter in the server decision is the type of load balancing scheme. The schemes currently supported are round robin, weighted round robin, and static.

A service, load balancing scheme and servers are associated by creating a load balancing group using the `lb-group` command.

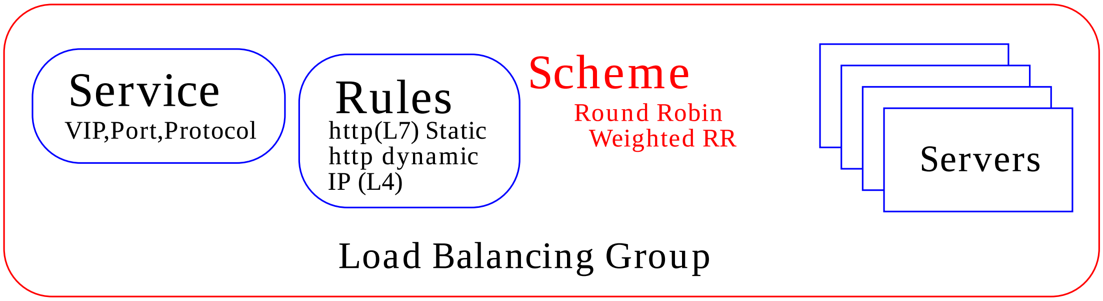

FIGURE 3 Load Balancing Group Configuration

For more details on command syntax for creating services, rules, and load balancing groups, refer to the *Sun Fire B10n Content Load Balancing Blade Administration Guide*.

Topology Fundamentals

To match the ample switching capacity of the SSC units in the Sun Fire B1600 blade platform the content load balancer solution is designed to direct server responses toward clients without passing through the content load balancer. This enables the outbound capacity of the system to scale in proportion to the number of servers deployed, and to exploit the natural web traffic asymmetry where most of the traffic is server outbound.

To combine the uncompromised Layer 7 service performance with the direct server response, the content load balancing blade relies on a software module in each server. This server module contributes to the solution’s high degree of integration by providing other key attributes, for example, path failover functionality.

The Sun Fire B1600 blade platform switches are separate networks, leaving the system designer the option to connect them externally and create a symmetrically configured redundant system where every blade is dual-homed, or to leave the switches segregated for a system where full redundancy is either not necessary (or achieved elsewhere in the system hierarchy), and blades are single-homed to separate networks. You can also create intermediate configurations where critical blades (content load balancers, proxies, and so on) reside on shelves with dual switches, but blade servers do not.

When you connect SSC switches to create redundant paths, it is best if:

- The interconnection occurs at the highest point in the network hierarchy
- The internal fabric of one shelf is connected directly to the corresponding fabric of another shelf (that is, daisy chain SSC0 with SSC0 and SSC1 with SSC1, and connect these uplinks at an external distribution switch, if any).

The above connections help ensure that the SSC switches are indeed leaf switches within the network infrastructure, and enable the content load balancer to use the shortest path within the redundant fabric (that is, the path that involves only one fabric).

FIGURE 4 illustrates nine shelves connected using a combination of distribution switches and internal SSC switches. Note that the SSC0 versus SSC1 fabric correspondence is preserved throughout the Layer 2 network, and that the fabrics are interconnected at the distribution switch level. In asymmetrical (capacity and hops) topologies like the one shown, it is also appropriate to house the content load balancing blades in shelves directly connected to the distribution switches.

Routers are shown for completeness as they represents the boundary of the Layer 2 network on the path towards the service clients.

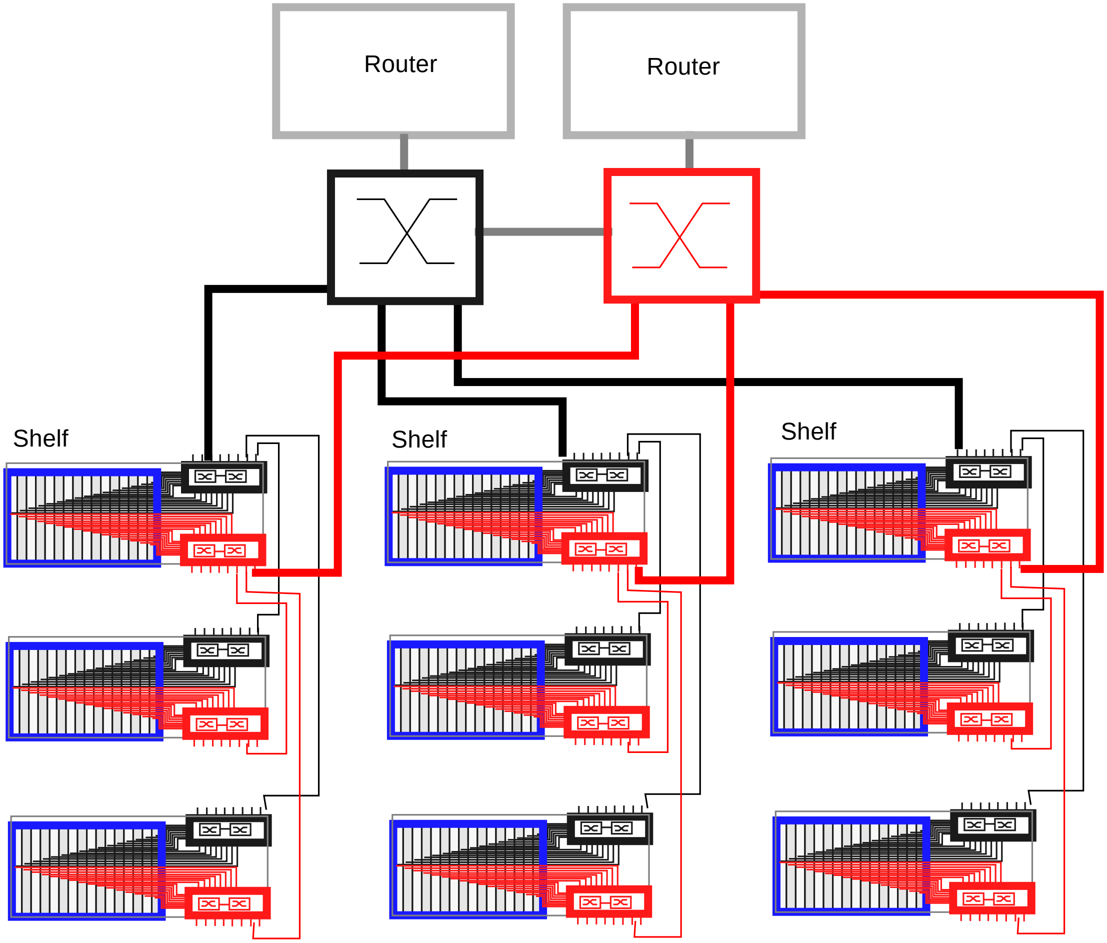

FIGURE 4 Sample Topology: Dual Tree Using External and Internal Switches

Load Balancing Terms

The following defines some common load balancing terms, and provides examples of their use.

Load Balancing Service

Defined by the destination 3-tuple, that is, the destination VIP, port, and protocol.

Example: 110.10.10.1:80:TCP

- Can be load balanced either at Layers 4 or 7
- Needs to be bound to one of the 2 interfaces on the blade
- Can be configured to support SSL if using a configuration with an SSL proxy
- When created, contains a default load balancing group with no servers or rules
- Load balancing groups with associated rules and schemes can be added
- Other attributes:
  - IP persistence
  - Cookie persistence
  - Tracking
  - Additional service access points (multi-homed service)

Load Balancing Group

- Contains a list of active servers (at least one)
- Contains a list of standby servers (optional)
- At least one rule must be specified (except for default group)
- Can add more rules or delete rules at run time
- Can add more servers or delete servers at run time
- Must have load balancing scheme specified:
  - Round Robin (RR)
  - Weighted Round Robin
  - Static Load Balancing

Load Balancing Rule

- A rule is associated with a load balancing group in a service
- Four types of rules:
  - Hypertext Transport Protocol (HTTP) URL rule

    Examples: `*.html`, `/subdir/*`, `/subdir/*.html`
  - CGI rule

    Example: `Server=MACHINE1`
  - Cookie rule

    Example: `L7server=server1`
  - IP rule

    Example: 129.47.29.0:2333/255.255.255.0:0

VLANs Optional for SSL Proxy Blades

The use of VLANs within the Sun Fire B1600 blade system is preferred when using the Sun Fire B10p SSL proxy blade. VLANs are configured at the SSC switches to create logical groups of endpoints that can communicate as if they were on the same LAN. VLANs also prevent or restrict traffic between endpoints on separate VLANs. However, some environments might not support VLANs. To disable VLAN operation for the Sun Fire B10p SSL proxy blade, use the `set vlan filter disable` command from the CLI interface.

If you choose to use VLANs, refer to the *Sun Fire B10n Content Load Balancing Blade Administration Guide* for detailed information.

Hardware and Software Requirements

Before using the Sun Fire B10n blade, ensure your system meets the hardware and software requirements listed in TABLE 3. If you need a server module for a later operating system release check the Sun Download Center at:

```
http://wwws.sun.com/software/download/network.html
```

TABLE 3 Hardware and Software Requirements

Hardware and Software	Requirements
Hardware	• Sun Fire™ B10n content load balancing blade • Sun Fire B10p SSL proxy blade (optional) • Sun Fire B1600 blade system chassis • Sun Fire B100s blade server for SPARC or Sun Fire B100x/B200x blade servers for x86 • Sun Fire V60/V65 and V210/V240 Servers (External to B1600 Chassis)
Software	• Sun Fire B10n content load balancing blade application software 1.2.3 or subsequent compatible version • Sun Fire B10n content load balancing blade BSC (blade support control) firmware v5.1.4* or subsequent compatible version

TABLE 3 Hardware and Software Requirements *(Continued)*

Hardware and Software	Requirements
Software *(Continued)*	• Sun Fire B100s Solaris Operating System versions: Solaris 8 HW 12/02 Solaris 8 HW 5/03 Solaris 8 HW 7/03 Solaris 8 HW 8/03 Solaris 9 8/03 Solaris 9 12/03 • Sun Fire V210/V240 Operating System versions: Solaris 8 HW 12/02 Solaris 8 HW 5/03 Solaris 8 HW 7/03 Solaris 8 HW 8/03 Solaris 9 8/03 Solaris 9 12/03 • Sun Fire B100x/B200x Operating System versions: x86 Solaris 9 12/03 Red Hat Advanced Server 2.1 Red Hat Advanced Server 2.1 Update 2 Red Hat Enterprise Linux 3.0 • Sun Fire V60/V65 Operating System versions: Solaris 9 8/03 Solaris 9 12/03 Red Hat Advanced Server 2.1 Red Hat Advanced Server 2.1 Update 2 Red Hat Enterprise Linux 3.0 • Sun Fire B1600 SC (system controller) 1.2 or subsequent compatible system controller firmware • B10n Solaris server module version v1.59 for Solaris, or B10n Linux server module version xxx1.41-1 for Red Hat Enterprise Linux AS 2.1.** • Sun GigaSwift Ethernet Adapter Patch ID 111883-18 or subsequent compatible patch for supported versions of the Solaris 8 software. Sun GigaSwift Ethernet Adapter Patch ID 112817-10 or subsequent compatible patch for supported versions of the Solaris 9 software.** • Sun Ethernet VLAN Patch ID 112119-04 or subsequent compatible patch for supported versions of the Solaris 8 software. Sun Ethernet VLAN Patch ID 114600-02 or subsequent compatible patch supported versions of the Solaris 9 software.***

* The version number displayed from the `showplatform -v` command from the Sun Fire B1600 SC CLI printout refers to the BSC firm-

ware version. The application software version is observed using the console `show version` command.

**Verify that you are using the supported Linux server module (xxx1.41-1) for the OS version on your Linux server.

***The patch currently installed can be displayed by entering `/usr/ccs/bin/mcs -p /platform/sun4u/kernel/drv/ce`. You can download patches from `http://sunsolve.sun.com`

Updating the B1600 System Controller

You can download the latest version of the `sc` firmware from the following web site:

`http://wwws.sun.com/software/download/network.html`

You need to set up a TFTP boot server to update the `sc` firmware. See the “Setting up a TFTP Server” section of the *Sun Fire B10n Content Load Balancing Blade Administration Guide.*

You can access all the Sun Fire B1600 documentation from the following web site:

`http://www.sun.com/products-n-solutions/hardware/docs/Servers/Workgroup_Servers/Sun_Fire_b100s/index.html`

▼ To Update the System Controller Firmware

1. **At the `sc` prompt, enter the following command:**

```
sc> flashupdate -s install server -f path SSCn/SC.
```

In the following example, 10.4.128.25 is the IP address for your TFTP boot server and `stiletto.1.1/c8/SunFireB1600-sc-v1.1.6.flashSSC0/SC` is the path to the file:

```
sc> flashupdate -s 10.4.128.25 -f stiletto.1.1/c8/SunFireB1600-sc-v1.1.6.flash
SSC0/SC
Warning: Are you sure you want to flashupdate the SSC0/SC flash image (y/n)? y
SSC0/SC: Preparing to flashupdate.
flashupdate: erasing segment 36 programming address ffedfffd
SSC0/SC: flashupdate complete.
```

2. **Reset the system using `resetsc` to load the new image.**

Updating B10n Application Software and BSC Firmware

It is important to verify that you have the latest software for the Sun Fire B10n content load balancing blade. Check the following web site for the latest software and documentation:

`http://wwws.sun.com/software/download/network.html`

You need to set up a TFTP boot server to update the `SC` firmware. See the “Setting up a TFTP Server” section of the *Sun Fire B10n Content Load Balancing Blade Administration Guide.*

You also need to configure the management IP address and default gateway address. Refer to the “Configuring the Networking” section of the *Sun Fire B10n Content Load Balancing Blade Administration Guide.*

Note – If you are updating both the B10n application software and BSC firmware, be sure to update the B10n application software *first*.

▼ To Update the B10n Application Software

With the B10n blade in the booted and running state perform the following steps:

1. **Access the Sun Fire B10n console. At the Sun Fire B1600 SC console `SC>` type:**

```
sc> console Sn
```

Where *n* is the slot number of the B10n blade

2. **Login to the B10n console.**

```
Login: admin
passwd: admin
```

3. **Verify the boot image and versions:**

```
puma{admin}# show system

Boot Options:
==============================================================================
Config Type   Config File   Boot Image   Diag Level   Verbose Mode
------------------------------------------------------------------------------
running              2      1 (1.2.3)              0         0
next                 2      1 (1.2.3)              0         0
0=============================================================================


Image Information Table:
========================================================================
Image  Blade  Image Type     Version    Build Date:Time  Size
------------------------------------------------------------------------
1      B10n   Load Balancer  1.2.3    12/05/03 : 14:53   4046868
2      B10n   Load Balancer  1.2.2    11/26/03 : 12:15   4045472
diag   B10n   Diagnostics    1.1.9    10/16/03 : 15:36   2410733
========================================================================

Flash FS /RFA0 free space = 13,033,472 bytes

puma{admin}#
```

The B10n software can be loaded with three different images and booted. The three images are `image 1`, `image 2`, and `diag`. These images denote software versions.

To load to image location 1, the blade expects image *filename* to be available in the TFTP server. Where *filename* is `sunfire_b10n.1.2.3`

4. **Determine which image to update (image 1 or 2), and update the empty or oldest image.**

5. **Update the B10n application software**

```
puma{admin}# update image
```

You can upgrade the software either interactively or noninteractively.

▼ To Update the Software Noninteractively

- **As admin, type the following command:**

```
puma{admin}# update image tftp server file image_name image location
```

The following image uses the TFTP server with the IP address of 192.50.50.201, the image name of `sunfire_b10n.1.2.3`, and the image at location 1.

```
puma{admin}# update image 192.50.50.201 file sunfire_b10n.1.2.3
image 1
```

The system returns the following output, verifying the parameters entered:

```
file exist! will overwrite /RFA0/BOOTIMAGE/boot_image_1
Start downloading sunfire_b10n.1.2.3... using TFTP
Transferring and writing to file /RFA0/BOOTIMAGE/boot_image_1...
please wait.

puma{admin}#
```

The following image uses the tftp server with the IP address of 192.50.50.201, the image name of `sunfire_b10n.1.2.3`, and the image at location `diag`.

```
puma{admin}# update image 192.50.50.201 file sunfire_b10n.1.2.3
image diag
```

The system returns the following output, verifying the parameters entered:

```
file exist! will overwrite /RFA0/BOOTIMAGE/boot_image_diag
Start downloading sunfire_b10n.1.2.2_diag... using TFTP
Transferring and writing to file /RFA0/BOOTIMAGE/boot_image_diag
.................................
please wait.

puma{admin}#
```

See the “To Update the Software Interactively” section of the *Sun Fire B10n Content Load Balancing Blade Version Administration Guide*.

▼ To Set the New Image to be the Default Image

1. **Configure the desired Boot Image. At the B10n console type:**

```
puma{admin}# config boot image x
```

Where *x* is the image you just updated

2. **Save the updated image using the** `commit` **command:**

```
puma{admin}# commit
commit : Are you sure to continue? [yes|no] yes
```

3. **Reboot to activate the new image:**

```
puma{admin} reboot

reboot: Are you sure to continue? [yes|no] yes
```

▼ To Update the BSC Firmware

1. **Escape to the system controller console by typing the pound sign (#) and period (.) in rapid succession:**

```
puma{admin} #.
```

Note – If the two characters are not typed in rapid succession nothing happens.

2. **At the** `sc` **prompt, check the current version of the BSC firmware:**

```
sc> showsc -v
FRU   Software Version            Software Release Date
-----------------------------------------------------------
S0    v5.1.4-SUNW,B10n,NetBlade1  Aug 12 2003 15:31:48
```

3. **At the** `sc` **prompt, enter the following command:**

```
sc> flashupdate -s TFTP_ip-addr -f filename Sn
```

Where *TFTP_ip-addr* is the TFTP server IP address, *n* is the slot number, *filename* is the file name of the image

In the following example, 192.50.50.201 is the IP address for your TFTP boot server and `/tftpboot/525-2018-05-t2.a37`:

```
sc> flashupdate -s 192.50.50.201. -f /tftpboot/525-2018-05-t2.a37 S12
```

4. **Reset the system using** `resetsc` **to load the new image.**

Replacing Your B10n Blade

The upgraded B10n blade has the following features:

1. The 1.0 BSC firmware
2. Two B10n boot images—version 1.0.1 and 1.1. The default boot image is 1.1.
3. The B10n bootrom, version 1.1.

▼ To Export the Configuration From the Old Board

1. **Go to the /RFA0 directory**

```
puma{admin}# cd /
```

2. **Tar the CONFIG directory:**

```
puma{admin}# tar lbconfig.tar CONFIG
```

3. **Export the config tar file:**

```
puma{admin}# export file
The FTP server address: <ftp_server_ip>
The source directory path: type [cr] to use current directory:
    (null) source path, using current directory
    The source file name: lbconfig.tar
    The destination directory path: <path_on_ftp_server>
The destination file name: lbconfig.tar
    The user name: <user_name_for_ftp_server>
The user password: <user_password_for_ftp_server>
export file succeed!
```

▼ To Import the Configuration to the Upgraded Board

1. **Power off the old board and remove it from the chassis.**

2. **Install the upgraded board.**

   The board comes up with an empty configuration with the B10n 1.1 application image running.

3. **Configure the network interface. Optionally, configure the management VLAN (if applicable).**

4. **Go to the /RFA0 directory:**

```
puma{admin}# cd /
```

5. **Import the 1.0 or 1.1 configuration:**

```
puma{admin}# import file
    The FTP server address: <ftp_server_ip>
The source directory path: <path_on_ftp_server>
The source file name: lbconfig.tar
    The destination directory path:
    (null) path, using current directory...
    The destination file name: lbconfig.tar
    The user name: <user_name_for_ftp_server>
The user password: <user_password_for_ftp_server>

import file succeed!
```

6. **Untar the configuration file.**

```
puma{admin}# untar lbconfig.tar
```

7. **Reboot the B10n blade to get the imported configuration:**

```
puma{admin}# reboot
```

Note – To run traffic with B10n 1.2 Update application image, the blade server module has to be updated to version 1.2 Update.

Updating Your Server

Use the appropriate instructions for updating your Solaris or Linux servers.

To Update the SPARC Solaris Server Module

1. **Download the 1.2 Update version of the server module software from the following site:**

   `http://wwws.sun.com/software/download/network.html`

2. **Unzip the file:**

```
# /usr/bin/unzip SunFire_B10n-1_2_Update-SolarisModule.zip
```

3. **Install the SPARC Solaris server module software packages:**

```
# cd path_to_unzipped_file/Solaris/sparc
# pkgadd -d .
```

4. **Restart the Solaris server module:**

```
# /etc/init.d/clbctl stop
# /etc/init.d/clbctl start
```

▼ To Update the x86 Solaris Server Module

1. **Download the 1.2 Update version of the server module software from the following site:**

   `http://wwws.sun.com/software/download/network.html`

2. **Unzip the file:**

```
# /usr/bin/unzip SunFire_B10n-1_2_Update-SolarisModule.zip
```

3. **Install the x86 Solaris server module software packages:**

```
# cd path_to_unzipped_file/Solaris/i386
# pkgadd -d .
```

4. **Restart the Solaris server module:**

```
# /etc/init.d/clbctl stop
# /etc/init.d/clbctl start
```

To Update the Linux Server Module

1. **Download the 1.2 Update version of the server module software from the following site:**

   http://wwws.sun.com/software/download/network.html

2. **Unzip the file:**

```
# /usr/bin/unzip SunFire_B10n-1_2_Update-LinuxModule.zip
```

   Different Linux OS subdirectories are available, such as, RHAS_2.1, SLES_8.0, ... additionally, hardware platforms such as B100x, B200x and V60_65x are available.

3. **Install the Linux server module for RHAS 2.1 Update 2, for example:**

```
# rpm -i sunclb-k2_4_9_e_24-1.41-1.i386.rpm
# rpm -i sunclb-admin-1.41-1.i386.rpm
```

4. **Restart the Linux server module:**

```
# /etc/init.d/clbctl stop
# /etc/init.d/clbctl start
```

To Upgrade the Linux Server Module From an Existing Installation

1. **Download the 1.2 Update version of the server module software from the following site:**

   http://wwws.sun.com/software/download/network.html

2. **Unzip the file:**

```
# /usr/bin/unzip SunFire_B10n-1_2_Update-LinuxModule.zip
```

   Different Linux OS subdirectories are available, such as, RHAS_2.1, SLES_8.0, ... additionally, hardware platforms such as B100x, B200x and V60_65x are available.

3. **Upgrade the Linux server module for RHAS 2.1 Update 2, for example:**

```
# rpm -U sunclb-k2_4_9_e_24-1.41-1.i386.rpm
# rpm -U sunclb-admin-1.41-1.i386.rpm
```

4. **Restart the Linux server module:**

```
# /etc/init.d/clbctl stop
# /etc/init.d/clbctl start
```

Known Problems With the Software

This section outlines the known problems with the current version of the software and describes workarounds to overcome these problems.

One Misconfigured Server Causes NPU Failure (Bug ID 5012865)

One failing server could cause an NPU failure on the B10n blade.

Work Around: Find and remove the failing server. Allow the B10n blade to remain in idle with no traffic for 10 to 30 minutes or untill you see that the cleanup counters (dump module analyze 10) are no longer counting up.

Combination of Application Monitoring and IP Persistence Does Not Work Correctly (Bug ID 4994130)

When IP persistence and application monitoring are configured for a service, the load balancer does not behave as expected.

When the monitored application on a server fails, but the server remains up, no new client will be sent to this server. However, clients that have connected to the server and whose persistence entry has not timed out will continue to be sent to the server. To them, the service may appear to be down.

Workaround: Do not configure IP persistence and application monitoring for the same service.

Output From the `show arp` Command

The following example shows a typical output from the `show arp` command:

```
LINK LEVEL ARP TABLE
destination      gateway            flags Refcnt  Use           Interface
--------------------------------------------------------------------------
192.50.50.11     00:03:af:26:73:07405    0       35330         iq0
192.50.50.12     00:03:af:26:97:fb405    1       16653         iq0
--------------------------------------------------------------------------
```

In the ARP table the gateway and flags columns are improperly shown. In the example above, `405` in the first line `should be aligned under the flags heading.`

Online Help Documentation Error (Bug ID 4900728)

Due to errors in Wind River's Rapid Control software, the following commands print the same output:

- `config no dns ?` and `config dns ?`
- `config no service ?` and `config service ?`
- `config no ssl ?` and `config ssl ?`
- `config no path-failover ?` and `config path-failover ?`

In addition, the correct syntax for these "`config no`" commands is as follows:

```
puma{admin}# config remove dns server ip-addr
puma{admin}# config remove service service-name
puma{admin}# config remove ssl
puma{admin}# config remove path-failover
```

Specific Sequence Required

System may panic if the content load balancing module (`clbmod`) is added to a "down" `ce` interface

Workaround

Be sure the ce interface is "up" before you load clbmod.

Note – If the B10n software from the Solaris 8 7/03 Software Supplement CD is loaded onto an unsupported platform and the system is rebooted, the following message is displayed: "can't load module: No such file or directory."

VIP Address Conflict (Bug ID 4910001)

If the load balancer VIP address is mistakenly used on another device, the other device broadcasts a gratuitous ARP and forces all of the clients and routers to learn that ARP entry.

Use the config vip-broadcast VIP-address mask command to force the load balancer to send a gratuitous ARP and force the clients and routers to relearn the VIP ARP entry as that of the load balancer.

Configuring VIP Addresses to be the Same as path failover Target IP Address (Bug ID 4907833)

This problem indicates a bad network configuration. The VIP address cannot be the same as the path failover target IP address. A future release will check for this condition.

Unknown Filter Edge [b9000010] (Bug ID 4925821)

An unknown filter edge occurs when the classifier.pm file in the config/config_x directory is corrupted. This should not happen during normal operation.

Workaround

Boot using the alternate configuration and remove the file config/config_x/classifier.pm where x is the configuration boot up that fails and has a value of 1 or 2.

Adding an SSL Service With a Duplicate Port (Bug ID 4908515)

When adding an SSL service, using the same VIP address with a different port, but the same SSL port is not allowed. The new SSL service must have a unique port number. For example, if an initial SSL service is running on SSL port 880, you must specify a different SSL port number for each new SSL service such as SSL port 881, 882, and so on.

Unknown Failover State With No Rules or Services (Bug ID 4925823)

If a blade failover system comes up with an unknown failover state and without any rules or services, one of the following might have caused it:

- You chose to skip the failover synchronization at boot time.
- The failover was stopped or disabled and then the failover configuration was saved to the following failover configuration file before reboot:

```
/RFA0/CONFIG/FAILOVER/config_x/failover/failover_cmd.conf
```

- Invalid information is stored in the following failover state information file:

```
/RFA0/CONFIG/FAILOVER/config_x/failover.state
```

Workaround

Remove the failover configuration from the system with the following commands as `admin` in config mode:

```
puma(config){admin}# config remove failover
puma(config){admin}# rm /RFA0/config/failover/config_x/failover/
failover_cmd.conf
```

Reboot the system.

If you still want to keep the blade failover configuration after the reboot, please refer to the “Configuring Failover” chapter in the *Sun Fire B10n Content Load Balancing Blade Version Administration Guide.*

Note – In all of the references to `config_x`, the 'x' is 1 or 2 depending on whether your load balancing is currently using configuration directory `config_1` or `config_2`.

Skipping the Failover Synchronization at Boot Time

At boot time, you have the option of skipping the blade failover synchronization. During boot the system prints the following message and waits for 5 seconds for you to respond:

```
Press Return key to skip the failover synchronization ...
```

`config no ip interface` *0|1*

If both interfaces of the B10n device are configured in the same subnet and if one of the interfaces is unconfigured, there might be loss of network connectivity from the B10n device. The device might not be able to switch all servers to the alternate interface. This can cause server/SSL devices to be marked down, and they will not be used in the load balancing.

Workaround

After unconfiguring the interface. Do a commit and then reboot the system.

Full Gallop Runs for Hours

The B10n software provides the following diagnostic tests:

```
PUMA Diagnostic Menu option:
=============================

Puma Memory Test(SDRAM)          r
Puma Loopback Test               l
Puma NPU Test                    n
Quit                             q
Specify the Test type :r
Memory Test



List of SDRAM Memory Test to run
================================

Marching Test            m
Gallop Test              g
MarchB Test              b
Quit                     q
Specify the Test type :g
Gallop Test
Valid Test Types BASIC | FULL | SPECIFY: FULL
*****Warning: Will Run for Hours.Suggest Running Overnight


Do You Still want to Continue [yes/no]:
```

Workaround

If you must use the Gallop test, be sure to run it at night or on a week end when the system is not in use.

Troubleshooting

You may notice the following behaviors, which might be interpreted as being problems. However, they are normal behaviors.

VIP Is Not Checked

If another system in the subnet is configured with the IP address used in the VIP of a service configured on B10n the networking for that system will not work because the clients and routers will learn one machine's MAC and the other machine will not receive any traffic on that VIP.

Workaround

Because this is normal behavior, the only workaround is to ensure that you do not use duplicate VIP addresses.

`commit` Allowed Though No Changes

The B10n software still allows the commit command even though no changes have been made to the configuration.

Workaround

This problem causes no ill effects, so it can be noted and ignored.

Server/SSL Does Not Respond to `ping` Even Though it is Marked as Up.

If both interfaces are configured in the same subnet then in some scenarios it is possible that the default route to a server/SSL device might be down and the devices might be unreachable (ping fails) from B10n, but the monitoring shows them as up.

This is not a bug. The monitoring will switch to the alternate interface and try to reach the device. `ping` will only try the one default interface.

Enterprise Example of Deploying VLANs

This section provides an example for configuring the Sun Fire B10n blade with VLANs in the enterprise. This section also provides a review of the VLAN capabilities of the Sun Fire B1600 blade platform and its components including B10n content load balancing blades and B10p SSL proxy blades. An example is provided using VLANs in a typical enterprise configuration including the commands to configure the individual components of the B1600 blade platform. Some knowledge of the B1600 blade platform and its components is required.

The enterprise model is used in this example because it best represents a common configuration and provides concepts that can be expanded or simplified as required. Because security is best deployed throughout the datacenter, this example describes how the B1600 blade platform and its components best fit into a large framework.

This section does not include details on the SSL or TLS security protocols. The SSL proxy blade offloads servers from compute intensive cryptographic processing and provides a secure centralized location for key and certificate administration and configuration. The decrypted traffic can be protected using VLANs and this section describes a suggested configuration for implementing a VLAN architecture.

The B1600 blade platform employs both logical and physical separation features to enable protection and isolation. The first level is the separation of management and data traffic. Management access can be attained either by direct Ethernet or serial connection to the System Service Controller (SSC) ports, or inband over the Ethernet switch fabric. The SSC uses a Layer 3 filter between the internal switch fabric and the system controller. An SSH agent is employed on the System Controller (SC) to provide authentication and cryptographic protection. The SSC is connected to each B1600 blade by redundant point to point serial connections providing an out of band path to each blade. Individual blade consoles can be accessed inband over the switch fabric as well. IEEE 802.1Q VLANs are available to logically separate the management traffic from the data traffic as well to segregate data traffic from different users.

When using the Sun Fire B10n content load balancing blade, traffic can be divided into load blancing groups and packets are forwarded based on services. Services can then be assigned a unique VLAN ID and the load balancer will tag traffic to the servers. If HTTPS is one of the types of traffic within a service, the Sun Fire B10p SSL proxy blade returns the decrypted ingress traffic to the B10n blade for the load balancing decision and will add the service VLAN tag before sending them to the server. When data leaves the servers headed for the client, the packets are tagged with the data VLAN ID, thus isolating this traffic from the service and management traffic. FIGURE 5 shows the configuration for this example and highlights the concepts described above.

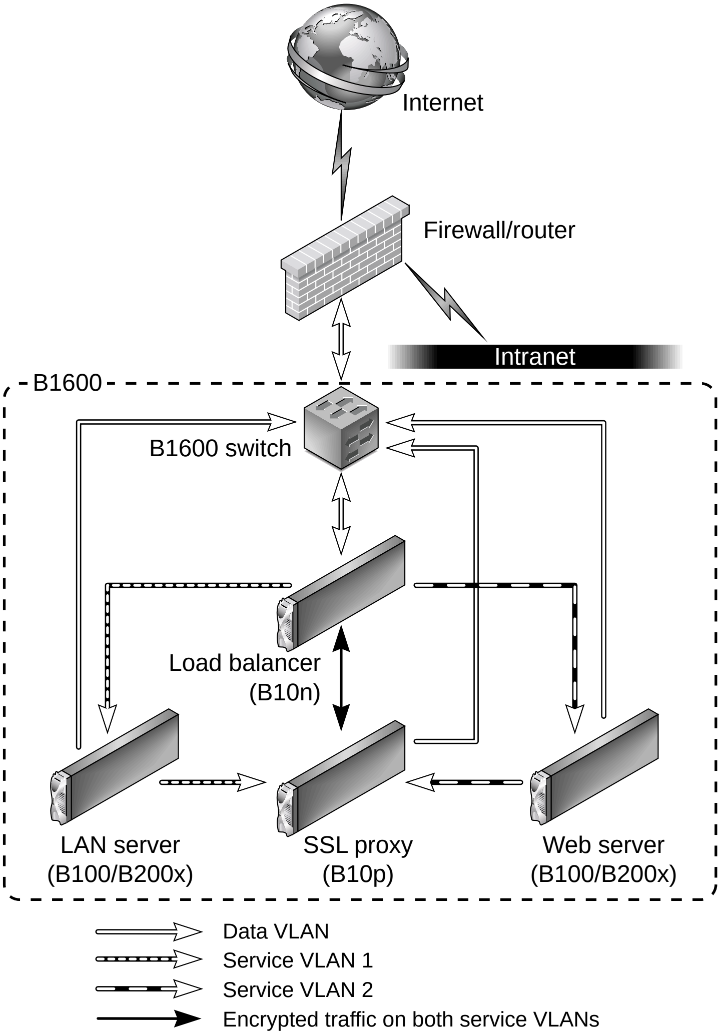

FIGURE 5 Enterprise Security Model

Once traffic leaves the B1600 switch toward the external network, the data VLAN tag can be either stripped or left and extended to the next hop router or firewall. Traffic ingress to the B1600 platform can be tagged by the router or firewall, or can be tagged by the SSC.

While the diagram above is useful in understanding the VLAN membership concepts and logical packet flow, it does not show the actual physical port connections. For example the load balancer has one physical interface per switch. Therefore the switch interface must be configured to allow all three VLANs in this example. This is true for the SSL proxy blade as well. The Server (or load balance group) interfaces must be configured with the management, data , and its service VLAN IDs. In this way this server is isolated from the other service traffic through the switches. It is important to know that the links between the blades and the switch are point to point; therefore, the switch VLAN filtering can prevent other VLAN traffic from being forwarded to a particular link.

User Access Control

User access levels are provided to restrict features from different administration users. The B1600 service controller allows multiple username and password accounts. Users are assigned up to four user access privileges types u, a, c, r which allow setting user accounts (u), administration of system controller configuration (a), console access to blades and switches (c), and the ability to power on/off blades and reset them (r).

Once you have console access, the server blades provide Unix access level options based on the type of OS you are running. In general root access is required to configure the VLAN parameters.

For the B10n content load balancing blade there are two levels: Level 1 is limited to read access to system information and status; Level 2 is full access.

The B10p SSL proxy blade employs three levels, *Service Officer (SO)* which provides full access, *Administrator* which allows access to the network configuration but does not allow access to keys or certificates, and the third is *User* which allows read access to some system information.

Definition of VLAN Terms

1. *Ingress* (RX) – Packets/Frames entering the device or network being described. In datacenter or server centric discussions sometimes referred to as client side or client traffic. That is, traffic transmitted by the client and received by the datacenter.

2. *Egress* (TX) – Packets/Frames leaving the local device or network. In datacenter or server centric discussions, it is traffic transmitted by the device or network and received by the client.

3. *Native* – Provided to allow network control traffic (like IGMP) to travel through VLAN enabled fabrics. From a switch perspective, untagged ingress packets are tagged with a specified value and egress packets with a specified ID are sent untagged.
4. *Allowed* – If ingress filtering is enabled, the switch will allow only tagged packets specified in the list for that port. If tagged is specified, it will leave tags on egress. If untagged is specified, it will strip tags on egress.
5. *GVRP* – VLAN Registration Protocol defines the way for switches to exchange information in order to automatically register members on interfaces across a network.

System Components and VLAN Attributes

B1600 Switch

IEEE 802.1Q – Up to 256 VLANs - GVRP and manual configuration

- Management Port – NETGMT [Default VLAN ID set to 2, Ingress filtering, Egress tagging]
- Native VLAN support [Default PVID set to 1 on NETP0-8 & SNP0-15 ports]
- Port Mode [Default Hybrid or can be set to Trunk]
- Ingress filtering (VLAN tag enforcement) [Default disabled]
- Ingress Tagging [packets are always tagged within the switch fabric]
- Egress Tagging [switchport allowed] (untagged – strip specified ID, tagged – leave specified ID)

Note – The B1600 switch supports Port and Hybrid VLAN configurations. All configurations in this example use Hybrid mode where tagged and untagged VLAN IDs are specified.

B10n Content Load Balancer

(Default is all VLANs disabled)

- Management VLAN (Default VLAN ID set to 2, Ingress Tag enforcement, Egress tagging, One Management VLAN per B10n)
- Data VLAN (Default VLAN ID is 1, Egress tagging for client bound packets, One Data VLAN per B10n)

- Service VLAN (One VLAN per Service, Egress replacement with Service VLAN ID)

B10p SSL Proxy

Role is to decrypt incoming SSL traffic and encrypt outgoing SSL.

(Default is VLANs enabled)

- Management VLAN (Default VLAN id set to 2, Ingress Tag enforcement, Egress tagging, One Management VLAN per B10p)
- Data VLAN (Default VLAN ID is 1, Ingress Tag enforcement, Egress replacement with Service VLAN ID)
- Service VLAN (Default VLAN ID is 1, Ingress Tag enforcement, Egress replacement with Data VLAN ID)

Server Blade

- Management VLAN [Ingress filtering (Tag enforcement), Egress tagging] (must be configured for B10n control and monitoring messages)
- Data VLAN (Ingress Tag enforcement, Egress Tagging)
- Service VLAN (Ingress Tag enforcement, Egress Data VLAN Tagging for client bound, Egress Service tagging for SSL clear text to Proxy.)

Enterprise Example

FIGURE 6 provides an example VLAN configuration of four VLANs.

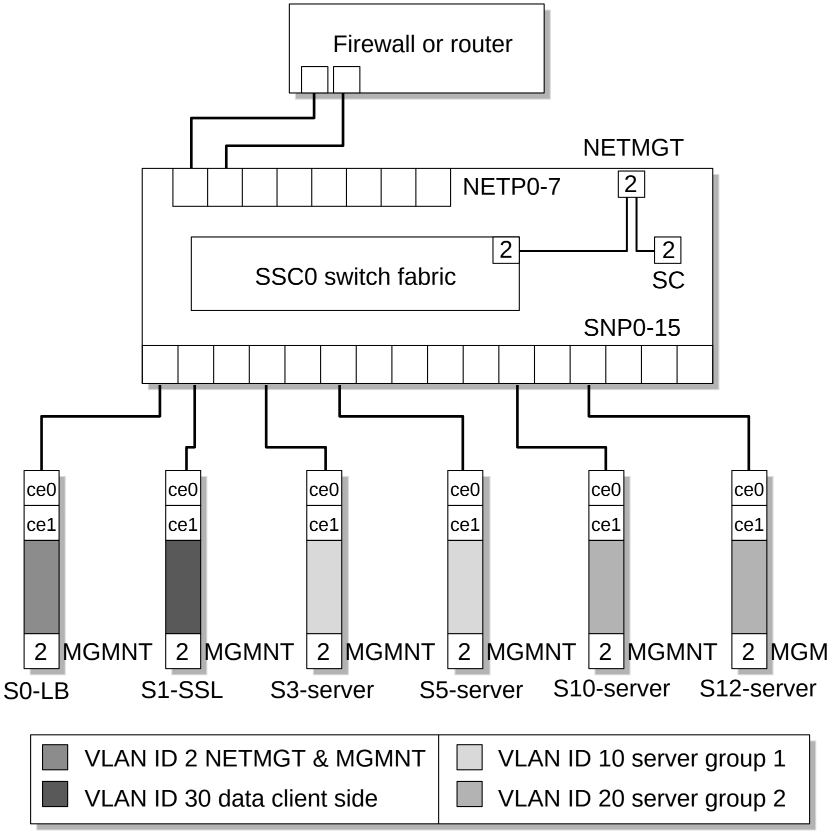

FIGURE 6 Enterprise Example

This enterpise example shows a physical view including network links, load balancer blade (LB), SSL proxy blade (SSL), and two server groups each with a unique service (SVC1 & SVC2). One for Internet access and the other for Intranet traffic. VLANs IDs are only shown for the end points of the management network as this is common to all blades and switch ports. The load balancer and SSL Interfaces must be a member of all four VLANs. The server interfaces are members of management, data, and a service VLAN. Below is a example of commands to configure the B1600 and its components based on FIGURE 6. The exception is that VLANs are not extended to the external firewall, but the switch is configured to untag the egress data VLAN packets and tag the ingress data VLAN packets.

The following four VLANs IDs are used.

1. Management VLAN ID 2
2. Data (or client side) VLAN ID 30
3. Service VLAN ID 10
4. Service VLAN ID 20

SSC VLAN Configuration

The first step to configure the system is configuring the VLANs for the SSC. The external network or “client side” uplink ports (NETPx), the internal (SNPx) ports, and the management ports configurations will be shown. The approach used for the uplink (NETPx) ports is to enable ingress filtering allowing only untagged VLAN IDs. The SSCs employ the concept of “native” VLANs which allow incoming untagged packets to be tagged with the VPID or native tag and untag egress packets that contain the VPID. The approach used for the internal (SNPx) ports is to allow both service VLANs as well as the management and data VLANs for the load balancer and SSL proxy blades. Server blade ports also allow management and data VLANs, but only one service VLAN is allowed. If all elements are in the same shelf, this contains the service VLANs (and thus cleartext and other service traffic) within the B1600. If external servers (or multiple shelves) are used, these VLANs can be extended by adding these VLAN IDs on those uplink ports connected to the additional servers or shelves. GVRP is used in this example.

The interfaces to be configured on the switch are:

- Management VLAN
- Uplink network ports
- Internal switch ports

For details on SSC switch configuration, refer to the *Sun Fire B1600 Blade System Chassis Switch Administration Guide.*

1. **Go to the SSC console from the SC prompt.**

```
sc>console sscn/swt
```

Where *n* is either 0 or 1 for systems with redundant switches.

2. **Type your user name and password.**

User access needs to at least have [a] administration privileges set.

```
Console#config
```

3. **Configure the Management port (this step can be skipped if default VLAN 2 has not been changed).**

```
Console(config)#interface ethernet NETMGT
Console(config)#switchport allowed vlan add 2
Console(config)#switchport native 2
Console(config)#switchport allowed vlan remove vlan id
```

Where *vlan id* is the previously configured value.

4. **Setup the VLAN database.**

```
Console(config)#vlan database
Console(config-vlan)#vlan 30 name external media ethernet
Console(config-vlan)#vlan 10 name loadgrp1 media ethernet
Console(config-vlan)#vlan 20 name loadgrp2 media ethernet
Console(config-vlan)#exit
```

5. **Configure the Uplink ports.**

```
Console(config)#interface ethernet netp0
Console(config-if)#no switchport gvrp
```

Note – By default the `gvrp` is disabled for all ports. Anytime you change the port configuration you must include the `no switchport gvrp` command to restore `gvrp`.

---

6. **Configure this uplink port to untag egress packets for these VLANs.**

```
Console(config-if)#switchport allowed vlan add 10,20,30 untagged
```

7. **Configure this uplink port to tag ingress untagged packets with this PVID.**

```
Console(config-if)#switchport native vlan 30
```

8. **Remove the default data VLAN.**

```
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#exit
```

Repeat this step for all uplink ports you want to include in the shared Data VLAN (30).

9. **Configure the internal port for the load balancer and SSL proxy blades.**

```
Console#config
Console(config)#interface ethernet snp0
Console(config-if)#switchport gvrp
Console(config-if)#switchport allowed vlan add 10 tagged
Console(config-if)#switchport allowed vlan add 20 tagged
Console(config-if)#switchport allowed vlan add 30 tagged
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#exit
```

Repeat the above instructions (10) for the SSL proxy changing `snp0` to `snp1`.

10. **Configure the internal ports for the servers.**

```
Console#config
Console(config)#interface ethernet snp3
Console(config-if)#switchport gvrp
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#switchport allowed vlan add 10 tagged
Console(config-if)#switchport allowed vlan add 30 tagged
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#exit
```

Repeat this sequence for the second server changing `snp3` to `snp5`.

Repeat this sequence for the second service group changing the firs allowed VLAN form 10 to 20.

The Load Balancer Service VLAN Configuration

The B10n load balancers must be a member of all four VLANs. The management VLAN must be the same for all blades to be load balanced as monitoring messages go between them and the B10n. The two services will be named SVC1 and SVC2 for the two load balancing groups.

The steps to configure VLANs on the B10n are as follows:

1. **Go to the B10n console from the SC prompt.**

```
sc>console sn
```

Where *n* is the slot number of the load balancing blade.

2. **Type your user name and password.**

User access privileges must be Level 2.

3. **Enter the B10n configuration mode.**

```
puma{admin}# config
```

4. **Set the management VLAN and enable.**

```
puma(config){admin}# management vlan 2
puma(config){admin}# enable vlan management
```

5. **Set the data VLAN and enable.**

```
puma(config){admin}# data vlan 30
puma(config){admin}# enable vlan data
```

6. **Set the service VLAN for SVC1 and enable.**

Note – The service SVC1 and SVC2 must be configured prior to these commands. Refer to the *Sun Fire B10n Content Load Balancing Administration Guide* for details.

```
puma(config){admin}# service vlan SVC1 vlan 10
puma(config){admin}# enable service vlan SVC1
puma(config){admin}# enable service name SVC1
```

7. **Set the service vlan for SVC2 and enable.**

```
puma(config){admin}# service vlan SVC2 vlan 20
puma(config){admin}# enable service vlan SVC2
puma(config){admin}# enable service name SVC2
puma(config){admin}# exit
```

8. **Verify the configuration.**

```
puma{admin}# show vlan
System VLAN Table:
==============================================================
VLAN Type VLAN ID      Status
------------------------------------------------------------------------------
Management                                 2            Enabled
Data   30           Enabled
==============================================================
Service VLAN Table:
==============================================================
Service Name VLAN ID      Status
------------------------------------------------------------------------------
SVC1                                       10           Enabled
SVC2                                       20           Enabled
==============================================================
```

The SSL Proxy Blade Configuration

The SSL proxy blade must be configured for all four VLANs. The default is VLANs are enabled. If the blade has been configured and you are just adding VLANs, you will begin by enabling VLANs.

1. **Access the SSL proxy blade console from the SC command line interface.**

```
sc>console sscn/swt
```

Where *n* is the slot number for the SSL proxy blade.

2. **Type your user name and password.**

User access needs to be Security Officer (SO) or Administrator (admin).

3. **Enable VLANs.**

```
CLI# set vlan filter enable
```

Note – Nonzero VLAN tags cannot be set before VLANs are enabled

---

4. **Configure the management VLAN.**

```
CLI# set vlan management 1 2
```

5. **Configure the data (client side) VLAN.**

```
CLI# set vlan client 30
```

6. **Configure the SVC1 service VLAN.**

```
CLI# set vlan inband 1 10
```

7. **Configure the SVC1 service VLAN.**

```
CLI# set vlan inband 2 20
```

8. **Verify the configuration.**

```
CLI# show vlan client
     client vlan:30

CLI# show vlan manage
     port 1:
       vlan:2
     port 2:
       vlan:2

CLI# show vlan inband
     port 1:
       vlan:10
     port 2:
       vlan:20

CLI# show vlan filter
     vlan filter: enabled
```

The Solaris Server VLAN Configuration

The command example here is for Solaris if Linux is being used the syntax will vary slightly but the concepts are the same.

The server must also be a member of three VLANs, the management, the data (client side), and the service VLAN. The management VLAN is used to exchange configuration and monitoring messages between the content load balancing blade and the blade server. The service VLAN is used for all data traffic between the content load balancing blade and the blade server.

The route from the server to the client network must use the data (client side) VLAN. For security reasons, the server cannot bind any services to its IP address on this interface.

- The management subnet is 192.50.50.0, with a mask of 255.255.255.0
- The IP address of the content load balancing blade is 192.50.50.10
- The IP address of the server on the management VLAN is 192.50.50.201
- The virtual IP address of the service is 199.99.9.1
- The default route is set to 10.10.10.10

1. **Go to the server blade console from the SC prompt.**

```
sc>console sn
```

Where *n* is the slot number of the server blade.

2. **Type your user name and password.**

   User access privileges must be superuser.

3. **Configure the data VLAN interface.**

```
# ifconfig ce30000 plumb 10.10.10.10 netmask 255.255.255.0 up
```

4. **Configure the management VLAN interface:**

```
# ifconfig ce2000 plumb 192.50.50.201 netmask 255.255.255.0 up
```

5. **Configure the SVC1 service VLAN interface:**

```
# ifconfig ce10000 plumb 150.10.10.10 netmask 255.255.255.0 up
```

6. **Configure the VIP on the loopback interface:**

```
# ifconfig lo0:1 plumb 199.99.9.1 netmask 255.255.255.0 up
```

   The IP address on the service VLAN is never used in any traffic; however, a valid IP address must be configured.

7. **Add all three interfaces to the load balanced interfaces:**

```
# /opt/SUNWclb/bin/clbconfig add ce2000
# /opt/SUNWclb/bin/clbconfig add ce10000
# /opt/SUNWclb/bin/clbconfig add ce30000
```

8. **Verify that the route to the default gateway uses interface** `ce30000`**.**

```
# netstat -r
```

   The `netstat -r` command displays the routing table, including the default route.

9. **Set the default route:**

```
# route add default 10.10.10.10 0
```

Remove any other default route shown by `netstat -r`. Note that there are other ways to set the default route to use this interface. Refer to the *Solaris Administration Guide*.

Note – If the physical interfaces used were connected to `ssc1`, the virtual interfaces would be `ce2001`, `ce10001`, and `ce30001`, respectively.

The interface number for VLAN *n* on physical interface *i* is determined by the following formula: 1000 * *n* + *i*

Hence, the interface name for VLAN 123 on physical interface `ce0` is `ce123000`

These steps need to be repeated for the other servers in the load balancing group. For the second load balancing group, the VIP must be different and the service VLAN changes from `ce10000` to `ce20000`.