



Multi-System High Availability Configuration Guide

Version #: XOS 9.5.1

Copyright and Trademark Information

Copyright© 2011 by Crossbeam Systems®

Boxborough, MA, USA

All Rights Reserved

The products, specifications, and other technical information regarding the products contained in this document are subject to change without notice. All information in this document is believed to be accurate and reliable, but is presented without warranty of any kind, expressed or implied, and users must take full responsibility for their application of any products specified in this document. Crossbeam Systems disclaims responsibility for errors that may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

This material is protected by the copyright and trade secret laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Crossbeam Systems), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Crossbeam Systems.

For permission to reproduce or distribute please contact your Crossbeam Systems account executive.

This product includes software developed by the Apache Software Foundation: www.apache.org.

Crossbeam, Crossbeam Systems, XOS, X-Series, X20, X30, X45, X60, X80, X80-S and any logos associated therewith are trademarks or registered trademarks of Crossbeam Systems, Inc. in the U.S. Patent and Trademark Office, and several international jurisdictions.

All other product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

Multi-System High Availability Configuration Guide	1
About This Guide	5
Intended Audience.....	5
Related Documentation.....	5
Software Documentation.....	5
Hardware Documentation.....	5
Conventions.....	6
Typographical Conventions.....	6
Cautions, Warnings, and Notes.....	7
Customer Support.....	8
Chapter 1: Configuring for High Availability	9
Overview of High Availability Mechanisms.....	9
High Availability Within an X-Series Chassis.....	9
High Availability on Multiple X-Series Chassis.....	10
Active-Standby Configuration.....	10
Active-Active Configuration.....	11
Failover Groups.....	11
Virtual Router (VR).....	11
VRRP Priority.....	11
High Availability (HA) Port and Management Interfaces.....	11
Configuring an Active-Standby High Availability System.....	12
Configuring an Active-Active High Availability System.....	15
Chassis Interconnection.....	18
Alarms.....	18
Chapter 2: Active-Standby VRRP Dual-Box High Availability Configuration	19
Chassis Hardware Configurations.....	19
Configuration Methods.....	20
Assumptions.....	20
Active-Standby Configuration.....	20
System Diagram (Active-Standby).....	21
1.0 Configuring Chassis 1.....	22
1.1 Configuring System-wide Parameters (Chassis 1).....	22
1.2 Configuring Failover Group 1 (Chassis 1).....	24
Configuring the virtual-router for the Gig16 circuit.....	25
Configuring the virtual-router for the Gig26 circuit.....	26
1.3 Optionally Configuring OSPF.....	27
1.4 Preemption.....	28
1.5 Management Circuit.....	28
1.6 Verifying Your Configuration.....	28
2.0 Configuring Chassis 2.....	31
2.1 Configuring System-wide Parameters (Chassis 2).....	31
2.2 Configuring Failover Group 1 (Chassis 2).....	33
Configuring the virtual-router for the Gig14 circuit.....	33
Configuring the virtual-router for the Gig24 circuit.....	34
2.3 Preemption.....	36
2.4 Management Circuit.....	36
2.5 Verifying Your Configuration.....	36
Chapter 3: Active-Active VRRP Dual-Box High Availability Configuration	39

Chassis Hardware Configurations	39
Assumptions	40
Active-Active Configuration	40
System Diagram (Active-Active)	41
1.0 Configuring Chassis 1	42
1.1 Configuring System-wide Parameters (Chassis 1)	42
1.2 Configuring Failover Group 1 (Chassis 1)	44
Configuring the virtual-router for the Gig13 circuit	45
Configuring the virtual-router for the Gig23 circuit	46
1.3 Optionally Configuring OSPF	48
1.4 Preemption	48
1.5 Management Circuit	48
1.6 Configuring Failover Group 2 (Chassis 1)	49
Configuring the virtual-router for the Gig18 circuit	49
Configuring the virtual-router for the Gig28 circuit	50
1.7 Preemption	52
1.8 Management Circuit	52
1.9 Verifying Your Configuration	53
2.0 Configuring Chassis 2	56
2.1 Configuring System-wide Parameters (Chassis 2)	56
2.2 Configuring Failover Group 1 (Chassis 2)	58
Configuring the virtual-router for the Gig12 circuit	59
Configuring the virtual-router for the Gig22 circuit	60
2.3 Optionally Configuring OSPF	62
2.4 Preemption	62
2.5 Management Circuit	62
2.6 Configuring Failover Group 2 (Chassis 2)	63
Configuring the virtual-router for the Gig17 circuit	64
Configuring the virtual-router for the Gig27 circuit	65
2.7 Preemption	67
2.8 Management Circuit	67
2.9 Verifying Your Configuration	67
Appendix A: Basic Chassis Configuration	71
Assign Hostnames	71
Assign a Domain Name	71
Glossary	73

About This Guide

This guide provides step-by-step instructions for creating high availability X-Series Platform configurations running XOS V9.0, XOS V9.0.1, XOS V9.5.0 or later.

This guide assumes that you have already installed the X-Series Platform hardware, and that you have a basic understanding of how the X-Series Platform is designed and operates.

IMPORTANT: For the latest updates and revisions to X-Series Platform documentation, log into the Crossbeam Online Support Portal at <http://www.crossbeam.com/support/online-support/>.

Intended Audience

This guide is intended for system integrators and other qualified service personnel responsible for installing and maintaining the Platform.

Related Documentation

The following documents are provided on the Crossbeam Systems USB Installer (USB I) or are available on the Crossbeam Systems Customer Support Web site located at <http://www.crossbeam.com/support/online-support/>.

Software Documentation

- *XOS Configuration Guide*
- *XOS Command Reference Guide*
- *XOS V9.5.1 Release Notes*
- *Install Server User Guide and Release Notes*
- *RSW Installation Guide* (available with the RSW kit, purchased separately) and *Release Notes*
- *Serialization Cookbook: IPS and Firewall*
- *Multi-System High Availability Configuration Guide*

Hardware Documentation

- *X20 and X30 Platform Hardware Installation Guide*
- *X60 Platform Hardware Installation Guide*
- *X80-S Platform Hardware Installation Guidex*
- *X-Series Module and FRU Installation Instructions (multiple documents)*

Conventions

Typographical Conventions

For paragraph text conventions, see [Table 1](#) on page 6.

For command-line text conventions, see [Table 2](#) on page 7.

Table 1. Typographical Conventions Used in Paragraph Text

Typographical Convention	Types of Information	Usage Examples
Bold	Elements on the graphical user interface.	In the IP Address field, type the IP address of the first VAP in the group. Click OK to close the dialog. Select the Print to File check box.
Courier	Keys on the keyboard. File names, folder names, and command names. Any information that you must type exactly as shown. Program output text.	Press <code>Esc</code> to return to the main menu. Save the <code>user.txt</code> file in the <code>user_install</code> directory. Use the <code>start</code> command to start the application. In the Username field, type <code>Administrator</code> . The XOS CLI <code>show calendar</code> command displays the system calendar: <code>Fri Mar 18 13:32:03 2011</code>
<i>Courier Italic</i>	File names, folder names, command names, or other information that you must supply.	In the Version Number field, type <code>8.5.patch_number</code> .
>	A sequence of commands from the task bar or menu bar.	From the taskbar, choose Start > Run . From the main menu, choose File > Save As... Right-click on the desktop and choose Arrange Icons By > Name from the pop-up menu.

Table 2. Typographical Conventions Used in Command-Line text

Typographical Convention	Types of Information	Usage Examples
Courier	User prompts and program output text.	CBS# show calendar Fri Mar 18 13:32:03 2011
Courier Bold	Information that you must type in exactly as shown.	[root@xxxxxx]# md crossbeam
< <i>Courier Italic</i> >	Angle brackets surrounding Courier italic text indicate file names, folder names, command names, or other information that you must supply.	[root@xxxxxx]# md <your_folder_name>
[]	Square brackets contain optional information that may be supplied with a command.	CBS# configure dns server <IP_address> [vap-group <VAP_group_name>]
	Separates two or more mutually exclusive options.	CBS# cp-unknown-state {cp1 cp2}
{ }	Braces contain two or more mutually exclusive options from which you must choose one.	CBS# configure vap-group <VAP_group_name> CBS(config-vap-grp)# raid {0 1}

Cautions, Warnings, and Notes



Caution: Lists precautions that you must take to avoid temporary data loss or data unavailability.



Warning: Lists precautions that you must take to avoid personal injury, permanent data loss, or equipment damage.

IMPORTANT: Lists important steps that you must perform properly or important information that you must take into consideration to avoid performing unnecessary work.

NOTE: Provides special information or tips that help you properly understand or carry out a task.

Customer Support

Crossbeam Systems offers a variety of service plans designed to meet your specific technical support requirements. For information on purchasing a service plan for your organization, please contact your account representative or see <http://www.crossbeam.com/support/technical-support/>.

If you have purchased a Crossbeam Systems product service plan and need technical assistance, you can report issues by telephone:

United States: +1 800-331-1338 OR +1 978-318-7595

EMEA: + 33 4 8986 0400

Asia Pacific: +1 978-318-7595

Latin America: +1 978-318-7595

You can also report issues via e-mail to support@crossbeam.com.

In addition, all of our service plans include access to the Crossbeam Customer Support Portal located at <http://www.crossbeam.com/support/online-support/>.

The Crossbeam Customer Support Portal site provides you with access to a variety of resources, including Customer Support Knowledgebase articles, technical bulletins, product documentation, and release notes. You can also access our real-time problem reporting application, which lets you submit new technical support requests and view all your open requests.

Crossbeam Systems also offers extensive customer training on all of its products. For current course offerings and schedules, please refer to the Crossbeam Education Services Web pages located at <http://www.crossbeam.com/support/training-services/>.

Configuring for High Availability

This chapter provides detailed information about setting up X-Series platforms to achieve the most common High Availability configurations. The following topics are covered in detail:

- [Overview of High Availability Mechanisms](#) 9
- [High Availability on Multiple X-Series Chassis](#) 10
- [Configuring an Active-Standby High Availability System](#) 12
- [Configuring an Active-Active High Availability System](#) 15
- [Chassis Interconnection](#) 18
- [Alarms](#) 18

Overview of High Availability Mechanisms

High Availability is implemented in several ways on X-Series chassis.

High Availability Within an X-Series Chassis

CPM Redundancy

Within an X-Series chassis, two CPMs can be configured to operate as a primary-secondary pair.

NOTE: On the primary chassis, a CPM failure triggers a VRRP failover to the secondary chassis that occurs in approximately 10 seconds. If you have configured the two CPMs in the primary chassis for redundant operation, the secondary CPM takes over in approximately one minute. If you have configured VRRP preemption between the master and backup failover groups, then when the secondary CPM becomes primary, a second failover occurs, back to the failover group on the initial chassis.

NPM Interface Redundancy

On an NPM, an interface can be defined as a backup to one or more master interfaces.

APM Redundancy

APMs can be configured in standby mode, ready to substitute for an APM that fails.

VAP groups that experience a VAP failure can be configured to preemptively acquire an APM from a lower-priority VAP group.

Disk Redundancy

On CPMs and APMs, pairs of disks can be configured in RAID 1 arrays.

NOTE: RAID 0 can also be configured on some CPMs and APMs, but by design, RAID 0 does not provide data redundancy.

High Availability on Multiple X-Series Chassis

Virtual Router Redundancy Protocol (VRRP)

Using VRRP, two or more X-Series chassis can be configured so that network traffic is re-routed from an active chassis to a standby chassis if a failure or unwanted change occurs on the primary chassis in any of the areas listed below. The failure decrements the VRRP priority of the associated VRRP failover group. If the size of the decrement lowers the VRRP priority below the VRRP priority of the associated failover group on the other chassis, a failover occurs.

- **Application Monitoring**

By default, any application that runs on VAP group that is part of a failover group is monitored. An application failure triggers a VRRP failover. No `priority-delta` is associated with this process.

- **Circuit**

Circuits can be configured as part of a Virtual Router. If the circuit goes down (for example, if it is disabled or if the associated interface fails), the VRRP priority of the associated failover group is decremented. The `priority-delta` that you specify determines whether a failover occurs.

NOTE: If a circuit is configured to stay up (for example, if the circuit is configured with the `link-state-resistant` parameter), the failure of the associated interface has no effect.

Circuits can also be configured independently from any Virtual Router. You can use the `monitor-circuit` command in the `conf-vrrp-group` context to monitor the circuit for failure. The `priority-delta` that you specify determines whether a failover occurs.

- **Interface** (physical or logical)

Interfaces can be monitored using the `monitor-interface` command in the `conf-vrrp-group` context. If the interface fails (for example, if the network device to which the interface is connected fails, or if the cable is unplugged), the `priority-delta` that you specify is applied.

- **VAP Group**

You can configure a VAP group as a member of one or more failover groups. You can configure the VAP group so that if the number of active VAPs falls below the value specified by the `active-vap-threshold` parameter, the `priority-delta` value is decremented. The result affects all failover groups to which the VAP group belongs.

- **Next Hop IP Address**

You can configure the `verify-next-hop-ip` command as part of the Virtual Router configuration. If the specified IP address cannot be reached, the `priority-delta` that you specify is applied.

- **Multi-Link Trunking Interface**

For a multi-link trunk interface, you can specify the number of individual interfaces that must be in the active state. If the number of active interfaces falls below this value, the `priority-delta` that you specify is applied.

Active-Standby Configuration

In an Active-Standby configuration, all of the traffic is handled by failover groups on the active X-Series chassis. Failover groups on the standby chassis handle no traffic until a failure lowers the priority of a traffic-handling failover group, at which time the corresponding failover group on the standby chassis assumes the primary role. Later, when the failure condition is resolved, the original roles may or may not be restored, depending on the configuration (see [Preemption](#) on page 67).

Active-Active Configuration

In an Active-Active configuration, failover groups on both X-Series chassis handle traffic. If a failure lowers the priority of any failover group sufficiently, the corresponding failover group on the other chassis takes over the traffic processing. When the failure condition is resolved, the traffic routing may or may not revert to what it was before the failure, depending on the configuration (see [Preemption](#) on page 67). Both chassis must have sufficient processing capacity to handle the total workload.

Failover Groups

Failover groups and Virtual Routers (VRs) are used only in High Availability configurations. A failover group is a grouping of one or more VRs. A VR identifies the circuits and associated VAP groups for high availability. Only a failover group, not the entire system or an individual VAP group, can fail over to a backup failover group on another system. Failover groups operate in pairs, one on each chassis, and are usually assigned different VRRP priorities. The failover group with the higher priority is the master.

NOTE: It is possible to assign the same priority to both failover groups in a pair. However, most users assign different priorities in order to define which group is to handle the traffic under normal operating conditions (when no failures have occurred).

Open Shortest Path First (OSPF) Cost

Another aspect of a failover involves the adjustment of certain parameters when a failover condition occurs. For example, the OSPF link cost associated with a failover group circuit can be increased when that group changes from master to backup. The Crossbeam Routing Software (RSW) then updates OSPF routes to ensure that traffic is routed through a circuit that is associated with the failover group that has become master.

Virtual Router (VR)

A virtual router can be attached to a single circuit only, and can include only one VAP group attached to that circuit. In addition, the VR can assign individual IP addresses to the circuit and the VAP group interface. For circuits already configured with an IP address, the VR can also assign a virtual IP address. This virtual IP address allows you to configure failover groups using the same virtual IP address on other systems.

VRRP Priority

Each failover group is assigned a VRRP priority. Typically, failover groups are defined in pairs and the failover group with the higher priority is designated the Master. Both failover groups in a pair must have the same ID and are usually configured with different VRRP priorities.

A failure within a chassis does not necessarily cause a failover from one failover group to another. Instead, the VRRP priority is reduced by a pre-configured value, called a priority-delta. Failover occurs only if the priority is reduced below the priority of the backup failover group. This minimizes or eliminates the problem of failing over to a chassis that has an even more diminished capacity. After any failure is rectified, the VRRP priority is increased by the same amount by which it was decremented when that failure occurred. When all failures are rectified, the priority returns to the originally configured value.

High Availability (HA) Port and Management Interfaces

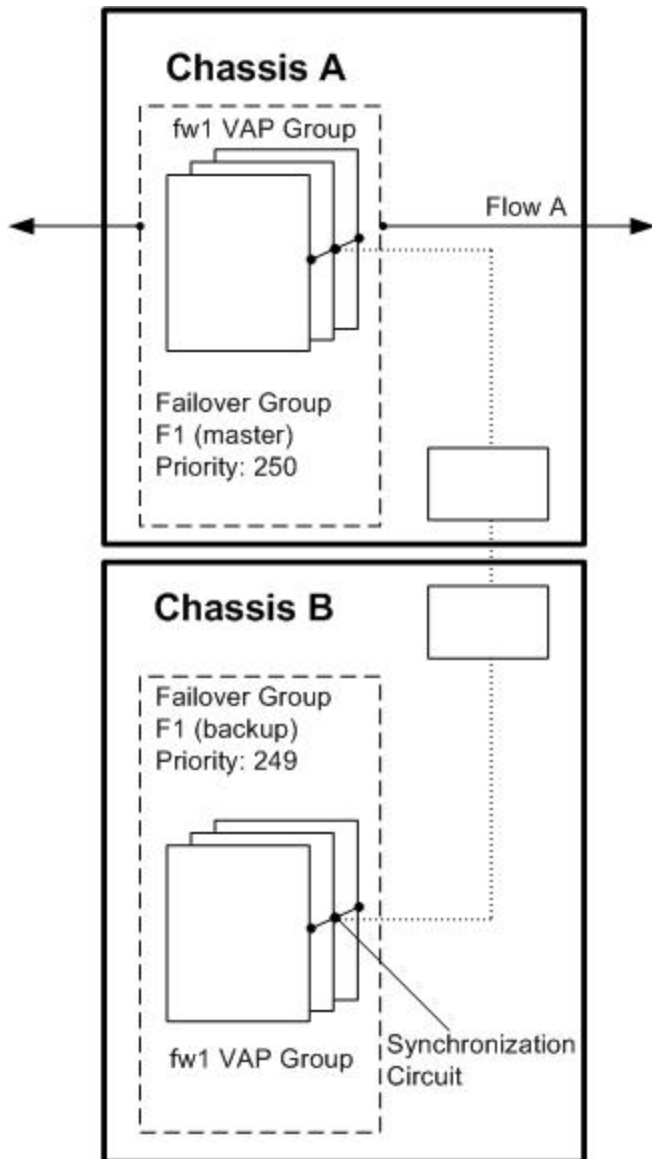
The X-Series Platform requires communication links between all the X-Series Platforms in a High Availability (HA) configuration. The High Availability, Management 1, and Management 2 ports provide these links. For details on how these ports should be connected, see [Chassis Interconnection](#) on page 18.

NOTE: Typically, you configure HA and Management ports for auto-negotiation. If you connect any of these ports to a switch and auto-negotiation does not work, use the `configure management high-availability` or `configure management gigabitethernet` command to manually set up the communication parameters.

Configuring an Active-Standby High Availability System

In an Active-Standby configuration, failover groups on one system are designated as master and process traffic and the corresponding failover groups on the other chassis are in standby mode. Each chassis has one or more failover groups configured. On each system, you attach one circuit to the virtual router in the local failover group. The most basic configuration, involving only one failover group, is shown in [Figure 1](#).

Figure 1. Active-Standby Configuration Before Failover



Chassis A:

On Chassis A, one failover group is associated with the fw1 VAP group.

Failover group F1 has a configured VRRP priority of 250 compared to a configured VRRP priority of 249 for the associated F1 failover group on Chassis B. As long as the current priority of the F1 failover group on Chassis A remains higher than the F1 failover group F1 on Chassis B, failover group F1 on Chassis A is designated as master and failover group F1 on Chassis B is standby.

Chassis A processes traffic through the fw1 VAP group until a failure occurs that lowers the VRRP priority of the F1 failover group below the VRRP priority of the associated F1 failover group on Chassis B. At that time, a failover occurs and the traffic that was being processed by the fw1 VAP group begins to be processed by the fw1 VAP group.

Chassis B:

On Chassis B, one failover group is associated with the fw1 VAP group.

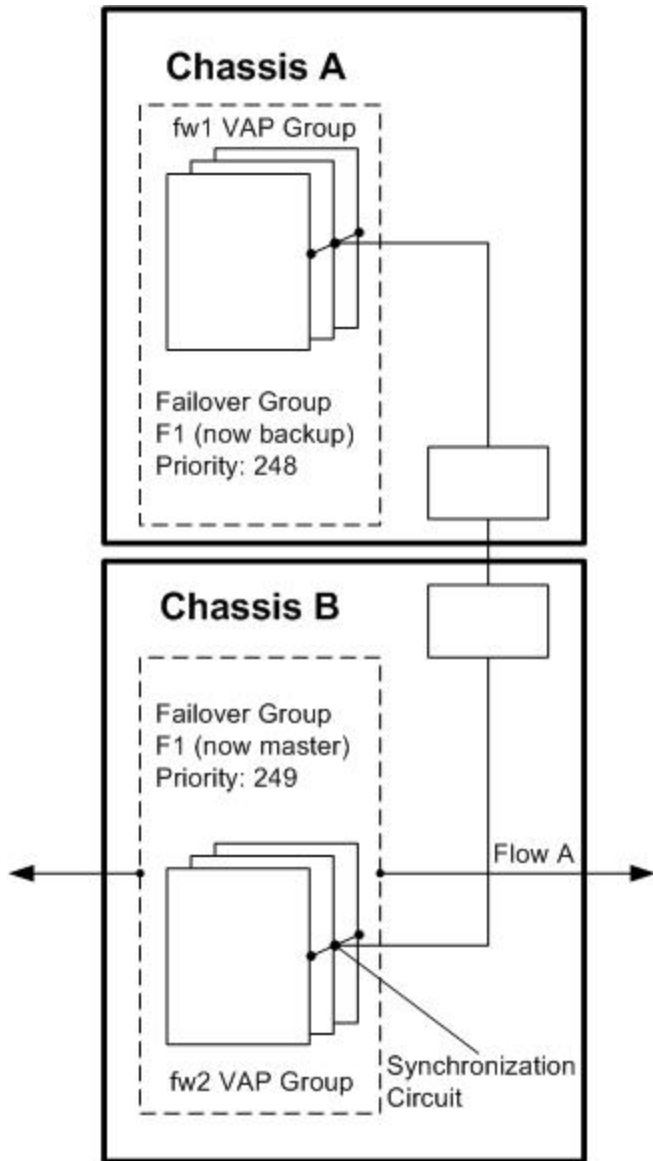
Failover group F1 has a configured VRRP priority of 249 compared to a configured VRRP priority of 250 for the associated F1 failover group on Chassis A. As long as the current priority of the F1 failover group on Chassis A remains higher than the F1 failover group F1 on Chassis B, failover group F1 on Chassis A is designated as master and failover group F1 on Chassis B is standby.

Chassis B does not process traffic until a failure occurs that lowers the VRRP priority of the F1 failover group on Chassis A below the VRRP priority of the associated F1 failover group on Chassis B. At that time, a failover occurs and the traffic that was being processed by the fw1 VAP group begins to be processed by the fw1 VAP group.

NOTE: When any failure occurs, the actual VRRP priority of the failover groups is compared, not the configured VRRP priority. If both chassis have experienced failures, the failover group with the higher actual priority is designated as master.

[Figure 2](#) on page 14 shows the configuration and traffic processing after a failure that has reduced the VRRP priority of the F1 failover group on Chassis A to 248.

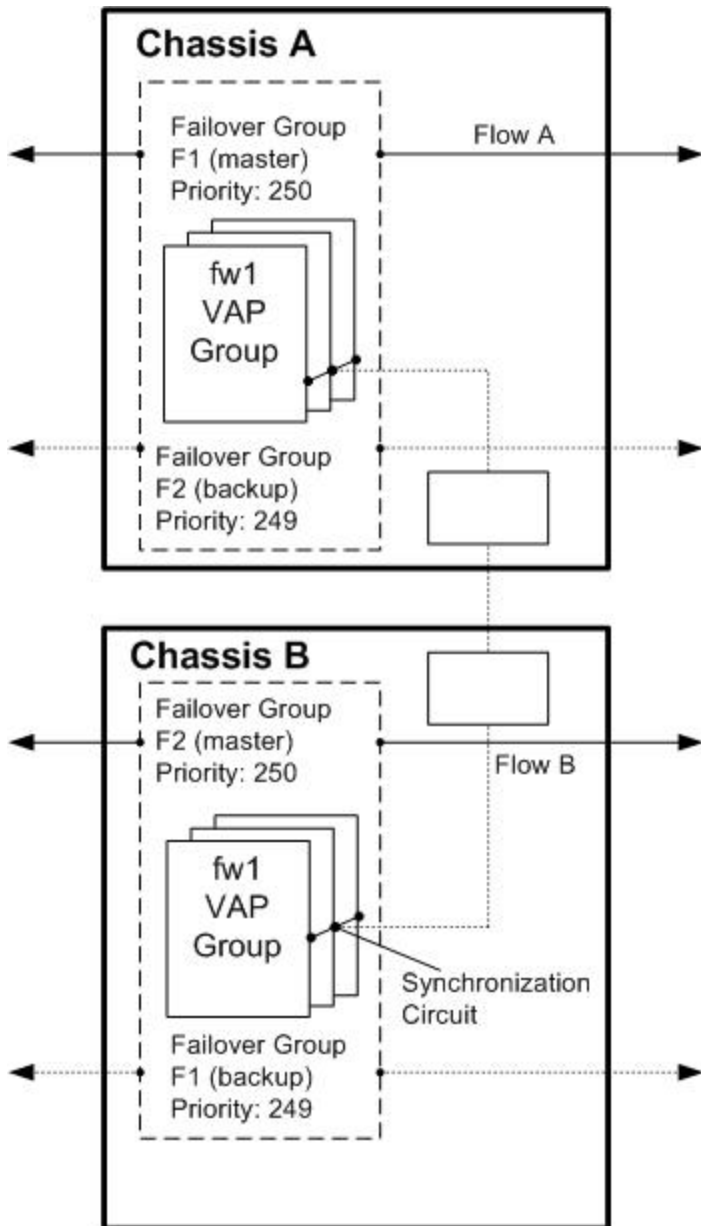
Figure 2. Active-Standby Configuration After Failover



Configuring an Active-Active High Availability System

In an Active-Active configuration, each system processes traffic and each has at least two failover groups configured. On each system, you attach one circuit to two Virtual Routers (VRs), where each VR is in a different failover group. The basic configuration, is shown in [Figure 3](#).

Figure 3. Active-Active Configuration Before Failover



Chassis A:

On Chassis A, two failover groups are associated with the fw1 VAP group.

Failover group F1 has a configured VRRP priority of 250 compared to a configured VRRP priority of 249 for the associated F1 failover group on Chassis B. As long as the current priority of the F1 failover group on Chassis A remains higher than the F1 failover group F1 on Chassis B, failover group F1 on Chassis A is designated as master and failover group F1 on Chassis B is standby.

Failover group F2 has a configured VRRP priority of 249 compared to a configured VRRP priority of 250 for the associated F2 failover group on Chassis B. As long as the current priority of the F1 failover group on Chassis A remains higher than the F1 failover group F1 on Chassis B, failover group F1 on Chassis A is designated as master and failover group F1 on Chassis B is standby.

Chassis A processes traffic through the fw1 VAP group until a failure occurs that lowers the VRRP priority of the F1 failover group below the VRRP priority of the associated F1 failover group on Chassis B. At that time, a failover occurs and the traffic that was being processed by the fw1 VAP group begins to be processed by the fw1 VAP group.

Chassis B:

On Chassis B, two failover groups are associated with the fw1 VAP group.

Failover group F1 has a configured VRRP priority of 249 compared to a configured VRRP priority of 250 for the associated F1 failover group on Chassis A. As long as the current priority of the F1 failover group on Chassis A remains higher than the F1 failover group F1 on Chassis B, failover group F1 on Chassis A is designated as master and failover group F1 on Chassis B is standby.

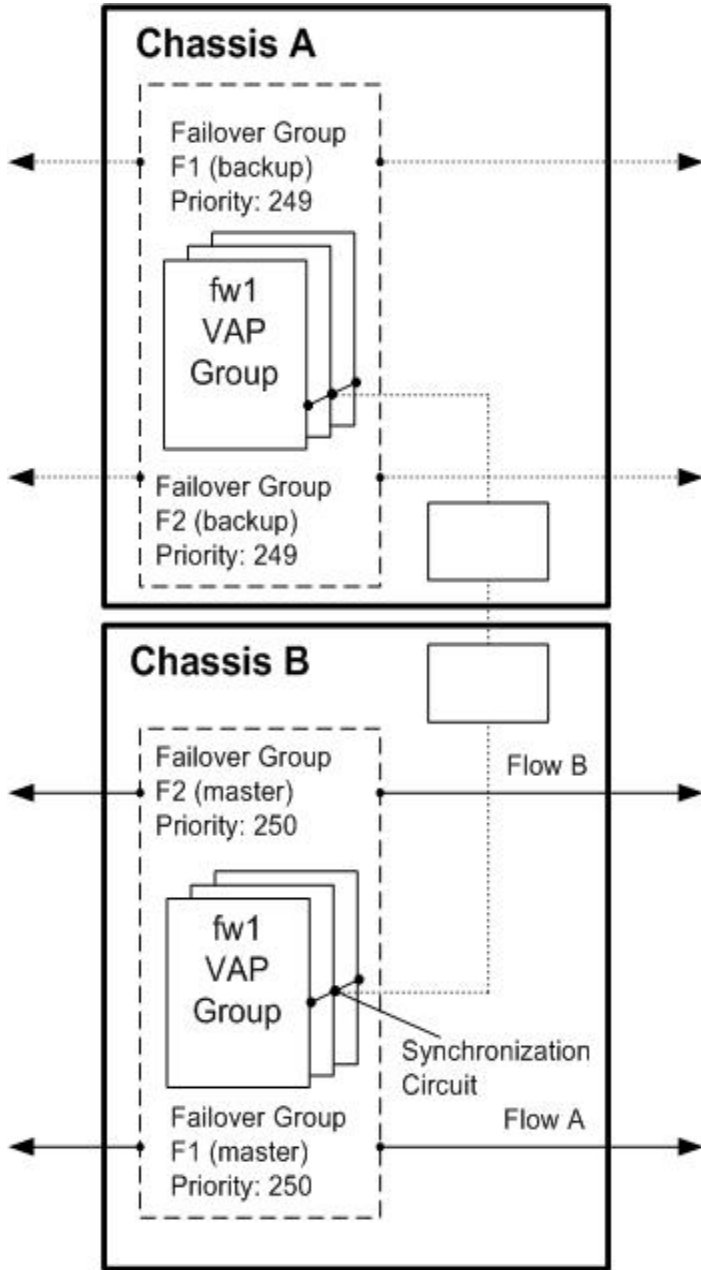
Failover group F2 has a configured VRRP priority of 250 compared to a configured VRRP priority of 249 for the associated F2 failover group on Chassis A. As long as the current priority of the F1 failover group on Chassis A remains higher than the F1 failover group F1 on Chassis B, failover group F1 on Chassis A is designated as master and failover group F1 on Chassis B is standby.

Chassis B processes traffic through the fw1 VAP group until a failure occurs that lowers the VRRP priority of the F2 failover group below the VRRP priority of the associated F2 failover group on Chassis A. At that time, a failover occurs and the traffic that was being processed by the fw1 VAP group begins to be processed by the fw1 VAP group.

NOTE: When any failure occurs, the actual VRRP priority of the failover groups is compared, not the configured VRRP priority. If both chassis have experienced failures, the failover group with the higher actual priority is designated as master.

[Figure 4](#) on page 17 shows the configuration and traffic processing after a failure that has reduced the VRRP priority of the F1 failover group on Chassis A to 150.

Figure 4. Active-Active Configuration After Failover to Chassis B



Chassis Interconnection

In a dual-chassis configuration where each chassis has a single CPM, Crossbeam recommends using the CPM High Availability (HA) port and both Management ports on the CPMs when connecting between chassis. The HA ports on the two CPMs can be connected directly or by means of a switch. The same is true for the Management ports; however, if switch connections are used, Crossbeam recommends that each pair of ports (HA, Management 1, and Management 2) be connected to separate switches.

In a dual-chassis configuration where each chassis has dual CPMs, Crossbeam recommends using both Management ports on the primary CPM and both Management ports on the secondary CPM when connecting between chassis. Each set of ports (Management 1, and Management 2) should be connected to separate switches. In the dual-CPM-per-chassis configuration Crossbeam recommends that customers do not connect the Management ports directly to each other.

NOTE: If the chassis have only a single connection, an alarm is generated. See [Alarms](#), next.

Alarms

Beginning with XOS V9.5.0, the XOS Alarm Subsystem has the ability to alert you about changes in status and problems with the configuration. Alarm information can be viewed using the Greenlight Element Manager (GEM), the CLI command `show alarms`, or by examining the system log files. Alarms also trigger SNMP traps.

Issues that can cause an alarm include:

- **Remote Box** — The configuration of any failover group on either chassis does not contain a definition for a remote box.
- **Failover Group Priority** — The priority of a failover group has changed.
- **Failover Group Status** — The status of a failover group has changed, possibly indicating that a failover has occurred.
- **Interconnection** — There is a problem with any of these paths between the local chassis and the remote chassis.
 - **No Active Path** — The Active Path (the path carrying the VRRP messages) between the chassis has failed. Typically, the Standby Path becomes the Active Path shortly after this failure has occurred.
 - **No Standby Path** — The Standby Path (the one that would become the Active Path if and when the Active Path failed) has failed.
 - **No Secondary Path** — The path to one of the management ports on the secondary CPM in the remote chassis has failed.
 - **Shared Interface** — All paths from the local chassis to the remote chassis share a single interface, creating a single point of failure.
 - **Path Status Change** — The status of one or more paths from the local chassis to the remote chassis has changed.
 - **XOS Mismatch** — The remote box is running an older version of the XOS software, in which the full DBHA functionality is not supported. Some errors may not be detected or reported.

Active-Standby VRRP Dual-Box High Availability Configuration

This chapter provides detailed information about setting up two X-Series platforms in an Active-Standby configuration. The Active platform processes traffic while the Standby platform is idle, ready to take over if the Active chassis experiences a problem.

Chassis Hardware Configurations

This chapter assumes the following:

Chassis 1 has the following hardware configuration:

- Internal network: 1.1.45.0/16 (System ID 45)
- Two CPMs
 - CP1 internal IP address: 1.1.45.20 (Primary)
 - CP2 internal IP address: 1.1.45.21 (Secondary)
- Four NPMs (NP1, NP2, NP3, and NP4)
- Eight APMs (AP3, AP4, AP5, . . . and AP10)
- Management Interface IP addresses:
 - 192.168.50.45 (Mgmt 13/1)
 - 192.168.51.55 (Mgmt 13/2)
 - 192.168.50.65 (Mgmt 14/1)
 - 192.168.51.75 (Mgmt 14/2)

NOTE: By default, CPM management interfaces are not configured but should be configured for dual-box high availability operation. The examples in this document include management interface information.

Chassis 2 has the following hardware configuration:

- Internal network: 1.1.46.0/16 (System ID 46)
- Two CPMs
 - CP1 internal IP address: 1.1.46.20 (Primary)
 - CP2 internal IP address: 1.1.46.21 (Secondary)
- Four NPMs (NP1, NP2, NP3, and NP4)
- Eight APMs (AP3, AP4, AP5, . . . and AP10)

- Management Interface IP addresses:
 - 192.168.50.46 (Mgmt 13/1)
 - 192.168.51.56 (Mgmt 13/2)
 - 192.168.50.66 (Mgmt 14/1)
 - 192.168.51.76 (Mgmt 14/2)

NOTE: By default, CPM management interfaces are not configured but should be configured for dual-box high-availability operation. The examples in this document include management interface information.

Configuration Methods

When you configure an Active-Standby system, you have these options.

- You can configure an IP address on the circuits and then assign the circuits to a Virtual Router.
- You can configure the circuits without IP addresses but assign an IP address to the associated Virtual Router.
- You can configure the system for Layer 2 operation, with no IP addresses.

This chapter uses the first of these methods.

Assumptions

This document assumes that:

- You have set up your two chassis for basic operation.
- Each chassis has a unique system ID.
- You have installed a Check Point firewall application.
- The two CPMs in each chassis are not configured for redundancy

For instructions on how to perform these tasks, see the list of documents in [Software Documentation](#) on page 5.

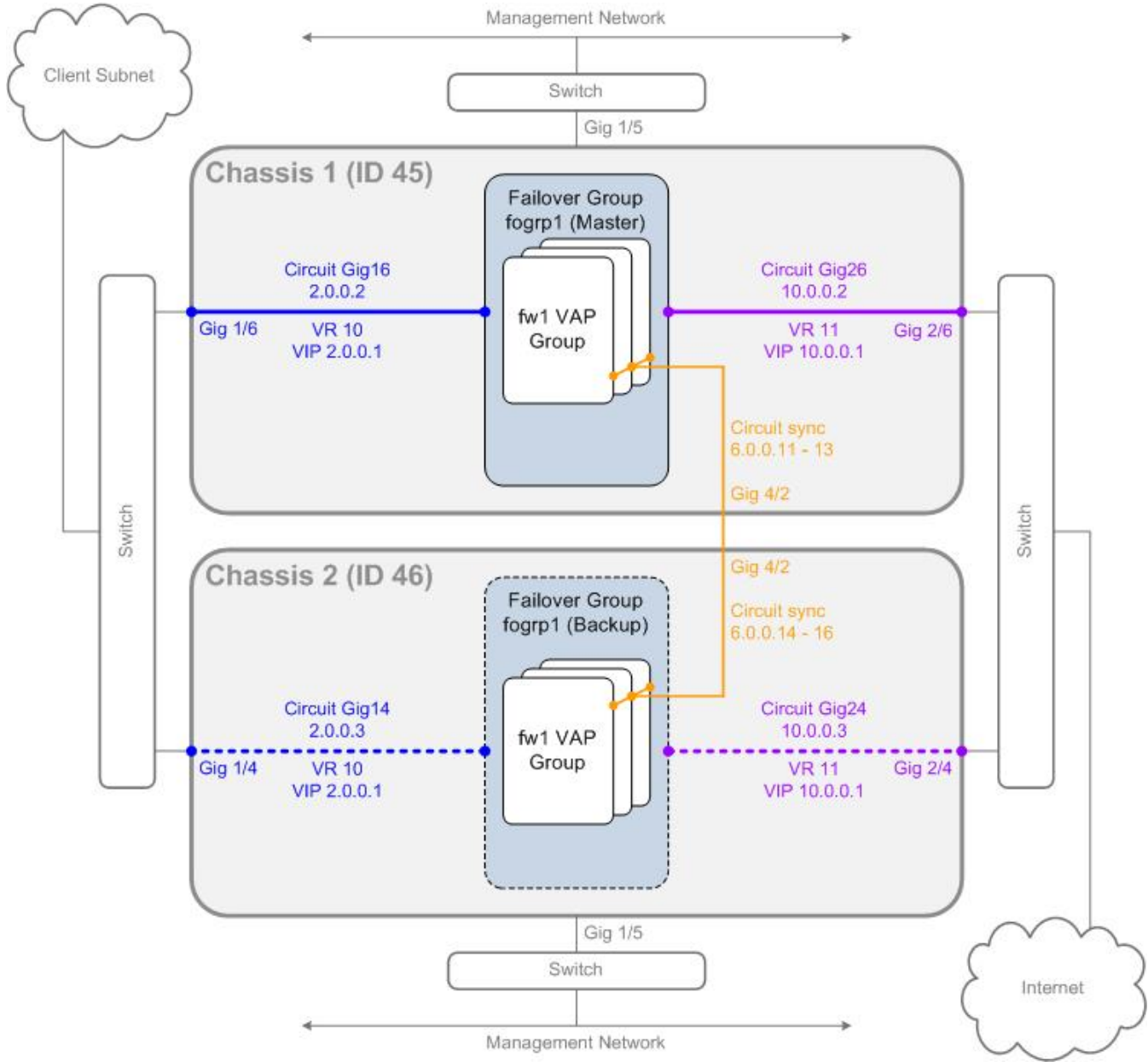
Active-Standby Configuration

This section describes how to configure the two chassis for Active-Standby VRRP Dual-box High Availability operation. See:

- [System Diagram \(Active-Standby\)](#) on page 21
- [Configuring Chassis 1](#) on page 22
- [Configuring Chassis 2](#) on page 31

System Diagram (Active-Standby)

This diagram illustrates the goal of the configuration steps in this chapter.



1.0 Configuring Chassis 1

On Chassis 1, perform these tasks:

- [Configuring System-wide Parameters \(Chassis 1\)](#) on page 22
- [Configuring Failover Group 1 \(Chassis 1\)](#) on page 24

1.1 Configuring System-wide Parameters (Chassis 1)

1.1.1 Local System Identifier

Configure the local `system-identifier` on Chassis 1.

NOTE: When configuring multiple chassis for high availability, a unique system ID must be assigned to each chassis. If both chassis are configured with the same ID, you run the risk of having identical MAC addresses on any given circuit. This configuration is **not** supported or recommended.

If your X-Series Platforms do not have unique system IDs assigned, use the following command to define a system ID. The valid range is from 1-255.

```
CBS# configure system-identifier 45
```

NOTE: After you configure the `system-identifier` parameter, you must use the `reload all` command to activate the identifier.

1.1.2 Remote System Identifier

NOTE: Crossbeam recommends that you connect the two chassis using the guidelines described in [Chassis Interconnection](#) on page 18, and then use the `configure remote-box` command on both chassis to configure ports on the remote chassis.

Configure the remote system ID and IP address using the `configure remote-box` command.

NOTE: The `configure remote-box` command requires that you have interconnected CPMs on the two chassis. Crossbeam recommends that you specify the following IP addresses:

- For the High Availability port, specify the **internal** IP address (1.1.46.20) associated with the remote Primary CPM (obtained by running `show internal-ip` on the remote chassis).
- For the management ports, specify the **external** IP addresses associated with the ports.

```
CBS# configure remote-box 46 1.1.46.20 192.168.50.46 192.168.51.56  
CBS(conf-remote-box) # end
```

NOTE: The example `configure remote-box` command specifies only the IP addresses of the management 1 and 2 interfaces and the internal IP address for the primary CPM on chassis 2. Crossbeam recommends that you connect the management interfaces of the other CPM on Chassis 2 and that you add the IP addresses for those interfaces to the `configure remote-box` command.

1.1.3 Configure the Synchronization Circuit

Configure a synchronization circuit between VAP Group fw1 on Chassis 1 and fw1 on Chassis 2 so that the two VAP Groups act as one Check Point Cluster with 6 members.

NOTE: This step must be performed **after** you configure the system ID, because the system ID affects the MAC selection and configuration of every circuit that gets created.

Enter these commands:

```
CBS# configure circuit sync
CBS(conf-cct)# device-name sync
CBS(conf-cct)# link-state-resistant
CBS(conf-cct)# vap-group fw1
CBS(conf-cct-vapgroup)# ip 6.0.0.11/24 increment-per-vap 6.0.0.13
CBS(conf-cct-vapgroup)# end
CBS#
CBS# configure interface gigabitethernet 4/2
CBS(conf-intf-gig)# logical sync
CBS(intf-gig-logical)# circuit sync
CBS(intf-gig-log-cct)# end
CBS#
```

1.1.4 Configure the Traffic Circuits

Configure the two circuits that convey traffic to and from the fw1 VAP group.

```
CBS# configure circuit Gig16
CBS(conf-cct)# device-name Gig16
CBS(conf-cct)# vap-group fw1
CBS(conf-cct-vapgroup)# ip 2.0.0.2/24
CBS(conf-cct-vapgroup-ip)# enable
CBS(conf-cct-vapgroup-ip)# end
CBS# configure circuit Gig26
CBS(conf-cct)# device-name Gig26
CBS(conf-cct)# vap-group fw1
CBS(conf-cct-vapgroup)# ip 10.0.0.2/24
CBS(conf-cct-vapgroup-ip)# enable
CBS(conf-cct-vapgroup-ip)# end
CBS#
```

1.1.5 Configure the Traffic Interfaces

Configure the interfaces through which traffic flows to and from the fw1 VAP group.

```
CBS# configure interface gigabitethernet 1/6
CBS(conf-intf-gig)# logical Gig16
CBS(intf-gig-logical)# circuit Gig16
CBS(intf-gig-log-cct)# end
CBS#
CBS# configure interface gigabitethernet 2/6
CBS(conf-intf-gig)# logical Gig26
CBS(intf-gig-logical)# circuit Gig26
CBS(intf-gig-log-cct)# end
```

1.2 Configuring Failover Group 1 (Chassis 1)

1.2.1 VRRP Failover Group

Create the failover group by assigning it a name (`fogrp1`) and a failover group ID. The failover group ID is different than the system identifier, configured earlier. The ID must be unique on this chassis, and must be the same on its counterpart failover group on the remote chassis (Chassis 2).

The `fogrp1` group acts as the master group on Chassis 1. The counterpart failover group on Chassis 2 is also called `fogrp1` and has the same group ID (1). The two groups have different priority values.

```
CBS# configure vrrp failover-group fogrp1 failover-group-id 1
CBS (conf-vrrp-group) #
```

1.2.2 VRRP Priority

For proper operation, the VRRP priority value of the two associated failover groups must be different on Chassis 1 and Chassis 2; during normal operations, the failover group with the higher priority is the master. Certain events such as an interface failure or a change in VAP group member count can be configured to decrement the VRRP priority of the failover group. Failover occurs when the VRRP priority value of one failover group drops below the priority of the failover group on the other chassis. VRRP priority values range from 1 to 255, and the default is 100.

```
CBS (conf-vrrp-group) # priority 250
CBS (conf-vrrp-group) # exit
```

1.2.3 Virtual Router on each Traffic Circuit

Create a virtual router on each traffic circuit that is attached to the `fw1` VAP group. A virtual router is assigned a virtual IP address that is used to configure VRRP and, optionally, next hop health check. This section describes the configuration of two virtual routers, one for each of the two circuits (`Gig16` and `Gig26`) that are associated with the `fw1` VAP group.

Configuring the virtual-router for the Gig16 circuit

1. To create the virtual router for the first circuit, enter this command.

```
CBS(conf-vrrp-group) # virtual-router vrrp-id 10 circuit Gig16
CBS(conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS(conf-vrrp-failover-vr) # priority-delta 2
CBS(conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's priority value is decremented by the `priority-delta` value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the priority value on Chassis 1 becomes 248, which is less than the priority value of the associated failover group on Chassis 2, so the failover group on Chassis 2 becomes the master. The `priority-delta` value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS(conf-vrrp-failover-vr) # mac-usage vrrp-mac
CBS(conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS(conf-vrrp-failover-vr) # vap-group fw1
CBS(conf-vrrp-vr-vapgroup) #
```

NOTE: Before you map the virtual router to the VAP group, the circuit must have been mapped to the VAP group. Mapping the VAP group to the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS(conf-vrrp-vr-vapgroup) # virtual-ip 2.0.0.1/24
CBS(conf-vrrp-vr-vapgroup) # end
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

Configuring the virtual-router for the Gig26 circuit

1. To create the virtual router for the second circuit, enter this command.

```
CBS (conf-vrrp-group) # virtual-router vrrp-id 11 circuit Gig26
CBS (conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS (conf-vrrp-failover-vr) # priority-delta 2
CBS (conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's priority value is decremented by the `priority-delta` value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the priority value on Chassis 1 becomes 248, which is less than the priority value of the associated failover group on Chassis 2, so the failover group on Chassis 2 becomes the master. The `priority-delta` value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS (conf-vrrp-failover-vr) # mac-usage vrrp-mac
CBS (conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS (conf-vrrp-failover-vr) # vap-group fw1
CBS (conf-vrrp-vr-vapgroup) #
```

NOTE: The circuit must already be mapped to the VAP group.

Specifying the VAP group of the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS (conf-vrrp-vr-vapgroup) # virtual-ip 10.0.0.1/24
CBS (conf-vrrp-vr-vapgroup) # end
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

1.2.4 Enable VRRP on the VAP Group

VRRP monitors the `fw1` VAP group for failure of individual VAPs. By setting the `active-vap-threshold` and the `priority-delta`, individual VAP failures can decrement VRRP priority and cause a comparison with the VRRP priority on the remote chassis. Failover occurs when the `priority-delta` value decrements the priority value of the master failover group below the priority value of the associated failover group on the remote chassis. In our configuration, the priority value for the master failover group is 250 and the priority value for the backup group is 249. A `priority-delta` of 2 is used for each of the VAP groups.

To configure the fw1 VAP group for failover:

1. Enable VRRP on the fw1 VAP group.

```
CBS# configure vrrp vap-group fw1
CBS (conf-vrrp-vap-group) #
```

2. Assign the VRRP enabled fw1 VAP group to a failover group list (required).

```
CBS (conf-vrrp-vap-group) # failover-group-list fogrpl
CBS (conf-vrrp-vap-group) #
```

3. Optionally, set the hold down timer.

Configure the hold-down-timer to 120, which forces the VAP group to wait for two minutes while the application fully boots. This wait prevents the failover group from becoming VRRP master before the application is fully active.

```
CBS (conf-vrrp-vap-group) # hold-down-timer 120
CBS (conf-vrrp-vap-group) #
```

4. Optionally, set the active VAP threshold and return to the main CLI context.

The active-vap-threshold monitors the number of active VAPs in the VAP group. If the number of active VAPs drops below the threshold, the failover group's priority value is decremented by the `priority-delta` (defined in the next step) and a comparison is done between the priorities of the failover groups on the two chassis. Failover occurs when the `priority-delta` decrements the priority value of the master failover group below the priority value of the backup group.

```
CBS (conf-vrrp vap-group) # active-vap-threshold 3
CBS (conf-vrrp vap-group) # end
CBS#
```

5. Set the `priority-delta` value for the VAP group (optional).

Assign a `priority-delta` to the VAP group. VRRP decrements the priority of the failover group whenever the number of active VAPs falls below the active-vap-threshold.

The `priority-delta` value can be any number between 1 and 255 and the default value is 1. When the VAP returns to the Active state, the `priority-delta` value is added back to the priority value.

```
CBS (conf-vrrp-vap-group) # priority-delta 2
CBS (conf-vrrp-vap-group) #
```

1.3 Optionally Configuring OSPF

If your network is configured to use the Open Shortest Path First (OSPF) protocol, you can incorporate OSPF into your VRRP configuration.

NOTE: To configure OSPF, you must first install the Crossbeam Routing Software (RSW).

When a failover occurs from one failover group to another, you want traffic to be rerouted from the failed group to the one that is now active. To ensure that this happens, you can increase the `ospf-cost-increment` value associated with the circuit on the first failover group. The new value is propagated to all local routers, increasing the OSPF cost of the circuit so that it is no longer part of the preferred route. When the original failover group resumes master status, the OSPF cost is readjusted to the originally configured value.

NOTE: Configure the `ospf-cost-increment` only on the master failover group.

To include OSPF cost in the configuration, perform these steps:

1. Configure these parameters on the master failover group (*fogrpl*):

```
CBS# configure vrrp failover-group fogrpl  
CBS (conf-vrrp-group) # ospf-cost-increment circuit Gig16 5  
CBS (conf-vrrp-group) # ospf-cost-increment circuit Gig26 5
```

2. On the VAP group that is associated with the master failover group, start the OSPF routing protocol.

```
CBS# configure routing-protocol ospf vap-group fw1 start
```

1.4 Preemption

Typically, after a failover has occurred from one failover group to another, you want the failover group that is now master to remain in that role, even after the problem that caused the failover has been resolved.

By default, preemption is turned off, and Crossbeam recommends that you do not configure preemption for failover groups.

However, if you want the original failover group to resume the role of master, you can turn preemption on using this command.

```
CBS (conf-vrrp-group) # preemption
```

1.5 Management Circuit

If you intend to run Check Point software on the X-Series chassis, do not configure the X-Series chassis management circuits as part of any failover group. This configuration is poor design and prevents access by the Check Point management station to the management circuit on the chassis on which the backup failover groups reside .

1.6 Verifying Your Configuration

This section contains the output of several commands that show the configured status of Chassis 1. To check your progress throughout the configuration process, open a second CLI window, log in to the CPM and enter one of the commands.

Output of show running-config on Chassis 1

```
CBS# show running-config  
#  
remote-box 46 1.1.46.20 192.168.50.46 192.168.51.56  
#  
vap-group fw1 xslinux_v5  
  vap-count 3  
  max-load-count 3  
  ap-list ap1 ap2 ap3 ap4 ap5 ap6 ap7 ap8 ap9 ap10  
  load-balance-vap-list 1 2 3 4 5 6 7 8 9 10  
  ip-flow-rule loadbalance1  
    action load-balance  
    activate  
#  
circuit Gig16 circuit-id 1025  
  device-name Gig16  
  vap-group fw1  
    ip 2.0.0.2/24 2.0.0.255
```

```

circuit Gig26 circuit-id 1026
  device-name Gig26
  vap-group fw1
    ip 10.0.0.2/24 10.0.0.255
circuit sync
  device-name sync
  link-state-resistant
  vap-group fw1
    ip 6.0.0.11/24 6.0.0.255 increment-per-vap 6.0.0.13
#
interface gigabitethernet 1/6
  logical Gig16
    circuit Gig16
interface gigabitethernet 2/6
  logical Gig26
    circuit Gig26
vrrp failover-group fogrp1 failover-group-id 1
  priority 250
  virtual-router vrrp-id 10 circuit Gig16
    priority-delta 2
    vap-group fw1
      virtual-ip 2.0.0.1/24 2.0.0.255
  virtual-router vrrp-id 11 circuit Gig26
    priority-delta 2
    vap-group fw1
      virtual-ip 10.0.0.1/24 10.0.0.255
#
vrrp vap-group fw1
  failover-group-list fogrp1
  hold-down-timer 120
  priority-delta 2
management gigabitethernet 13/1
  ip-addr 192.168.50.45/24 192.168.50.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 13/2
  ip-addr 192.168.51.55/24 192.168.51.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 14/1
  ip-addr 192.168.50.65/24 192.168.50.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 14/2
  ip-addr 192.168.51.75/24 192.168.51.255
  enable
  access-list 1 input
  access-list 2 output

```

Output of show vrrp on Chassis 1

```
CBS# show vrrp
Priority is Actual/Configured
FG-ID Priority Status Preempt Master Sys ID Master Priority
1      250/250 Master off      45                250
(1 row)
```

Output of show vrrp detail-status on Chassis 1

```
CBS# show vrrp detail-status
FG_ID Status Priority Delta Type Component
1 Master 250/250 2 vr Gig16/10/5
1 Master 250/250 2 vr Gig26/10/5
1 Master 250/250 2 vg fw1
```

NOTE: The Component column shows 5 as the last digit only if you configured the OSPF cost increment as described in [Optionally Configuring OSPF](#) on page 27. If you did not configure the OSPF cost increment, these values would be 0 (zero).

Output of show remote-box on Chassis 1

```
CBS# show remote-box
Local System ID: 45

Remote System ID: 46
Remote IP      Local Intf  Local IP      Status  Time In State  Link Qual
192.168.50.46  14/1       192.168.50.45 Active   9 days, 03:10  100
192.168.51.56  14/2       192.168.51.55 Active   9 days, 02:07  100
1.1.46.20      HA port    1.1.45.20     Active   9 days, 02:07  100
(3 rows)
```

2.0 Configuring Chassis 2

On Chassis 2, perform these tasks:

- [Configuring System-wide Parameters \(Chassis 2\)](#) on page 31
- [Configuring Failover Group 1 \(Chassis 2\)](#) on page 33

2.1 Configuring System-wide Parameters (Chassis 2)

2.1.1 Local System Identifier

Configure the local `system-identifier` on Chassis 2.

IMPORTANT: When configuring multiple chassis for high availability, a unique system ID must be assigned to each chassis. If both chassis are configured with the same ID, you run the risk of having identical MAC addresses on any given circuit. This configuration is **not** supported or recommended.

If your X-Series Platforms do not have system IDs assigned, use the following command to define a system ID. The valid range is from 1-255.

```
CBS# configure system-identifier 46
```

NOTE: After you configure the `system-identifier` parameter, you must use the `reload all` command to activate the identifier.

2.1.2 Remote System Identifier

NOTE: Crossbeam recommends that you connect the two chassis using the guidelines described in [Chassis Interconnection](#) on page 18, and then use the `configure remote-box` command on both chassis to configure ports on the remote chassis.

Configure the remote system ID and IP address using the `configure remote-box` command.

NOTE: The `configure remote-box` command requires that you have interconnected CPMs on the two chassis. Crossbeam recommends that you specify the following IP addresses.

- For the High Availability port, specify the **internal** ip address (1.1.45.20) associated with the remote Primary CPM (obtained by running `show-internal-ip` on the remote chassis).
- For the management ports, specify the **external** IP address(es) associated with the port(s).

```
CBS# configure remote-box 45 1.1.45.20 192.168.50.45 192.168.51.55
CBS(conf-remote-box) # end
```

NOTE: The example `configure remote-box` command specifies only the IP addresses of the management 1 and 2 interfaces and the internal IP address for the primary CPM on chassis 1. Crossbeam recommends that you connect the management interfaces of the other CPM on Chassis 1 and add the IP addresses for those interfaces to the `configure remote-box` command.

2.1.3 Configuring the Synchronization Circuit

Configure a synchronization circuit between VAP Group fw1 on Chassis 1 and fw1 on Chassis 2 so that the two VAP Groups act as one Check Point Cluster with 6 members.

NOTE: This step must be performed **after** you configure the system ID, because the system ID affects the MAC selection and configuration of every circuit that gets created.

Enter these commands:

```
CBS# configure circuit sync
CBS (conf-cct) # device-name sync
CBS (conf-cct) # link-state-resistant
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 6.0.0.14/24 6.0.0.255 increment-per-vap 6.0.0.16
CBS (conf-cct-vapgroup) # end
CBS#
CBS# configure interface gigabitethernet 4/2
CBS (conf-interface-gig) # logical sync
CBS (intf-gig-logical) # circuit sync
CBS (intf-gig-log-cct) # end
CBS#
```

2.1.4 Configure the Traffic Circuits

Configure the two circuits that convey traffic to and from the fw1 VAP group.

```
CBS# configure circuit Gig14 device-name Gig14
CBS# configure circuit Gig14 vap-group fw1
CBS (conf-cct-vapgroup) # ip 2.0.0.3/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS# configure circuit Gig24 device-name Gig24
CBS# configure circuit Gig24 vap-group fw1
CBS (conf-cct-vapgroup) # ip 10.0.0.3/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS#
```

2.1.5 Configure the Traffic Interfaces

Configure the interfaces through which traffic flows to and from the fw1 VAP group.

```
CBS# configure interface gigabitethernet 1/4
CBS (conf-intf-gig) # logical Gig14
CBS (intf-gig-logical) # circuit Gig14
CBS (intf-gig-log-cct) # end
CBS#
CBS# configure interface gigabitethernet 2/4
CBS (conf-intf-gig) # logical Gig24
CBS (intf-gig-logical) # circuit Gig24
CBS (intf-gig-log-cct) # end
```

2.2 Configuring Failover Group 1 (Chassis 2)

2.2.1 VRRP Failover Group

Create the failover group by assigning it a name (`fogrp1`) and a failover group ID. The failover group ID is different than the system identifier, configured earlier. The ID must be unique on this chassis, and must be the same on its counterpart failover group on the remote chassis (Chassis 1).

The `fogrp1` group on Chassis 2 acts as the backup group to the `fogrp1` group on Chassis 1. The two groups have different priority values.

```
CBS# configure vrrp failover-group fogrp1 failover-group-id 1
CBS (conf-vrrp-group) #
```

2.2.2 VRRP Priority

For proper operation, the VRRP priority value of the two associated failover groups must be different on Chassis 1 and Chassis 2; during normal operations, the failover group with the higher priority is the master. Certain events such as an interface failure or a change in VAP group member count can be configured to decrement the VRRP priority of the failover group. Failover occurs when the VRRP priority value of one failover group drops below the priority of the failover group on the other chassis. VRRP priority values range from 1 to 255, and the default is 100.

```
CBS (conf-vrrp-group) # priority 249
CBS (conf-vrrp-group) #
```

2.2.3 Virtual Router on each Traffic Circuit

Create virtual routers on each traffic circuit that is attached to the `fw1` VAP group. A virtual router is assigned a virtual IP addresses that is used to configure VRRP and, optionally, next hop health check. This section describes the configuration of two virtual routers, one for each of the two circuits (`Gig14` and `Gig24`) that are associated with the `fw1` VAP group.

Configuring the virtual-router for the Gig14 circuit

1. To create the virtual router for the first circuit, enter this command.

```
CBS (conf-vrrp-group) # virtual-router vrrp-id 10 circuit Gig14
CBS (conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS (conf-vrrp-failover-vr) # priority-delta 2
CBS (conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's priority value is decremented by the `priority-delta` value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the priority value on Chassis 2 becomes 247, which remains less than the priority value of the associated failover group on Chassis 1, so the failover group on Chassis 1 remains master. The `priority-delta` value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS (conf-vrrp-failover-vr) # mac-usage vrrp-mac
CBS (conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS (conf-vrrp-failover-vr) # vap-group fw1
CBS (conf-vrrp-vr-vapgroup) #
```

NOTE: Before you map the virtual router to the VAP group, the circuit must have been mapped to the VAP group.

Mapping the VAP group to the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS (conf-vrrp-vr-vapgroup) # virtual-ip 2.0.0.1/24
CBS (conf-vrrp-vr-vapgroup) # end
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

Configuring the virtual-router for the Gig24 circuit

1. To create the virtual router for the second circuit, enter this command.

```
CBS (conf-vrrp-group) # virtual-router vrrp-id 11 circuit Gig24
CBS (conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS (conf-vrrp-failover-vr) # priority-delta 2
CBS (conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's priority value is decremented by the `priority-delta` value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the priority value on Chassis 2 becomes 247, which remains less than the priority value of the associated failover group on Chassis 1, so the failover group on Chassis 1 remains master. The `priority-delta` value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS (conf-vrrp-failover-vr) # mac-usage vrrp-mac
CBS (conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS (conf-vrrp-failover-vr) # vap-group fw1
CBS (conf-vrrp-vr-vapgroup) #
```

NOTE: The circuit must already be mapped to the VAP group.

Specifying the VAP group of the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS (conf-vrrp-vr-vapgroup) # virtual-ip 10.0.0.1/24
CBS (conf-vrrp-vr-vapgroup) # end
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

2.2.4 Enable VRRP on the VAP Group

VRRP monitors the fw1 VAP group for failure of individual VAPs. By setting the `active-vap-threshold` and the `priority-delta`, individual VAP failures can decrement VRRP priority and cause a comparison with the VRRP priority on the remote chassis. Failover occurs when the `priority-delta` decrements the `priority` value of the master failover group below the priority value of the associated failover group on the remote chassis. In the example configuration, priority for the master failover group is 250 and priority for the backup group is 249. A `priority-delta` of 2 is used for each of the VAP groups.

To configure the fw1 VAP group for failover:

1. Enable VRRP on the fw1 VAP group.

```
CBS# configure vrrp vap-group fw1
CBS (conf-vrrp-vap-group) #
```

2. Assign the VRRP enabled fw1 VAP group to a failover group list (required).

```
CBS (conf-vrrp-vap-group) # failover-group-list fogrp1
CBS (conf-vrrp-vap-group) #
```

3. Optionally, set the hold down timer.

Configure the `hold-down-timer` to 120, which forces the VAP group to wait for two minutes while the application fully boots. This wait prevents the failover group from becoming VRRP master before the application is fully active.

```
CBS (conf-vrrp-vap-group) # hold-down-timer 120
CBS (conf-vrrp-vap-group) #
```

4. Optionally, set the active VAP threshold and return to the main CLI context.

The `active-vap-threshold` monitors the number of active VAPs in the VAP group. If the number of active VAPs drops below the threshold, the failover group's `priority` value is decremented by the `priority-delta` (defined in the next step) and a comparison is done between the priorities of the failover groups on the two chassis. Failover occurs when the `priority-delta` decrements the `priority` value of the master failover group below the priority value of the backup group.

```
CBS (conf-vrrp vap-group) # active-vap-threshold 3
CBS (conf-vrrp vap-group) # end
CBS#
```

5. Set the `priority-delta` value for the VAP group (optional).

Assign a `priority-delta` to the VAP group. VRRP decrements the priority of the failover group whenever the number of active VAPs falls below the `active-vap-threshold`.

The `priority-delta` value can be any number between 1 and 255 and the default value is 1. When the VAP returns to the Active state, the `priority-delta` value is added back to the `priority` value.

```
CBS (conf-vrrp-vap-group) # priority-delta 2
CBS (conf-vrrp-vap-group) #
```

2.3 Preemption

Typically, after a failover has occurred from one failover group to another, you want the failover group that is now master to remain in that role, even after the problem that caused the failover has been resolved.

By default, preemption is turned off, and Crossbeam recommends that you do not configure preemption for failover groups.

However, if you want the original failover group to resume the role of master, you can turn preemption on using this command.

```
CBS (conf-vrrp-group) # preemption
```

2.4 Management Circuit

If you intend to run Check Point software on the X-Series chassis, do not configure the X-Series chassis management circuits as part of any failover group. This configuration is poor design and prevents access by the Check Point management station to the management circuit on the chassis on which the backup failover groups reside .

2.5 Verifying Your Configuration

This section contains the output of several commands that show the configured status of Chassis 2. To check your progress throughout the configuration process, open a second CLI window, log in to the CPM and enter one of the show commands.

Output of show running-config on Chassis 2

```
CBS# show running-config
#
remote-box 45 1.1.45.20 192.168.50.45 192.168.51.55
#
vap-group fw1 xslinux_v5
  vap-count 3
  max-load-count 3
  ap-list ap1 ap2 ap3 ap4 ap5 ap6 ap7 ap8 ap9 ap10
  load-balance-vap-list 1 2 3 4 5 6 7 8 9 10
  ip-flow-rule loadbalance1
    action load-balance
    activate
#
circuit Gig14 circuit-id 1025
  device-name Gig14
  vap-group fw1
  ip 2.0.0.3/24 2.0.0.255
circuit Gig24 circuit-id 1026
  device-name Gig24
  vap-group fw1
  ip 10.0.0.3/24 10.0.0.255
circuit sync
  device-name sync
  link-state-resistant
  vap-group fw1
  ip 6.0.0.14/24 6.0.0.255 increment-per-vap 6.0.0.16
#
interface gigabitethernet 1/4
  logical Gig14
  circuit Gig14
```

```

interface gigabitethernet 2/4
  logical Gig24
  circuit Gig24
#
vrrp failover-group fogrpl failover-group-id 1
  priority 249
  virtual-router vrrp-id 10 circuit Gig14
  priority-delta 2
  mac-usage vrrp-mac
  vap-group fw1
    virtual-ip 2.0.0.1/24 2.0.0.255
  virtual-router vrrp-id 11 circuit Gig24
  priority-delta 2
  mac-usage vrrp-mac
  vap-group fw1
    virtual-ip 10.0.0.1/24 10.0.0.255
#
vrrp vap-group fw1
  failover-group-list fogrpl
  hold-down-timer 120
  priority-delta 2
#
management gigabitethernet 13/1
  ip-addr 192.168.50.46/24 192.168.50.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 13/2
  ip-addr 192.168.51.56/24 192.168.51.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 14/1
  ip-addr 192.168.50.66/24 192.168.50.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 14/2
  ip-addr 192.168.51.76/24 192.168.51.255
  enable
  access-list 1 input
  access-list 2 output

```

Output of show vrrp on Chassis 2

```

CBS# show vrrp
Priority is Actual/Configured
FG-ID  Priority  Status  Preempt  Master Sys ID  Master Priority
1      249/249    Backup  off      45             250
(1 row)

```

Output of show vrrp detail-status on Chassis 2

```

CBS# show vrrp detail-status
FG_ID  Status  Priority  Delta  Type  Component
1      Backup  249/249  2      vr    Gig14/10/0
1      Backup  249/249  2      vr    Gig24/11/0
1      Backup  249/249  2      vg    fw1

```

Output of show remote-box on Chassis 2

```
CBS# show remote-box  
Local System ID: 46
```

```
Remote System ID: 45
```

Remote IP	Local Intf	Local IP	Status	Time In State	Link Qual
192.168.50.45	14/1	192.168.50.46	Active	9 days, 03:10	100
192.168.51.55	14/2	192.168.51.56	Active	9 days, 02:07	100
1.1.45.20	HA port	1.1.46.20	Active	9 days, 02:07	100

(3 rows)

Active-Active VRRP Dual-Box High Availability Configuration

This chapter provides detailed information about setting up two X-Series chassis in an Active-Active VRRP Dual-box High Availability configuration. Each chassis has two failover groups, one of which is configured as master and processes traffic. The other failover group is configured as backup for the master failover group on the other chassis. Both chassis process traffic and, if either one experiences a problem, the backup failover group on the other chassis becomes master, and the other chassis assumes the workload of both.

Chassis Hardware Configurations

This chapter assumes the following:

Chassis 1 has the following hardware configuration:

- Internal network: 1.1.45.0/16 (System ID 45)
- Two CPMs
 - CP1 internal IP address: 1.1.45.20 (Primary)
 - CP2 internal IP address: 1.1.45.21 (Secondary)
- Four NPMs (NP1, NP2, NP3, and NP4)
- Eight APMs (AP3, AP4, AP5, . . . and AP10)
- CPM Management Interface IP addresses:
 - 192.168.50.45 (Mgmt 13/1)
 - 192.168.51.55 (Mgmt 13/2)
 - 192.168.50.65 (Mgmt 14/1)
 - 192.168.51.75 (Mgmt 14/2)

NOTE: By default, CPM management interfaces are not configured but should be configured for dual-box high availability operation. The examples in this document include management interface information for illustration purposes.

Chassis 2 has the following hardware configuration:

- Internal network: 1.1.46.0/16 (System ID 46)
- Two CPMs
 - CP1 internal IP address: 1.1.46.20 (Primary)
 - CP2 internal IP address: 1.1.46.21 (Secondary)
- Four NPMs (NP1, NP2, NP3, and NP4)
- Eight APMs (AP3, AP4, AP5, . . . and AP10)

- Management Interface IP addresses:
 - 192.168.50.46 (Mgmt 13/1)
 - 192.168.51.56 (Mgmt 13/2)
 - 192.168.50.66 (Mgmt 14/1)
 - 192.168.51.76 (Mgmt 14/2)

NOTE: By default, CPM management interfaces are not configured but can be configured if desired. The examples in this document include management interface information for illustration purposes.

Assumptions

This document assumes that:

- You have set up your two chassis for basic operation.
- Each chassis has a unique system ID.
- You have installed a Check Point firewall application.
- The two CPMs in each chassis are not configured for redundancy

For instructions on how to perform these tasks, see the list of documents in [Software Documentation](#) on page 5.

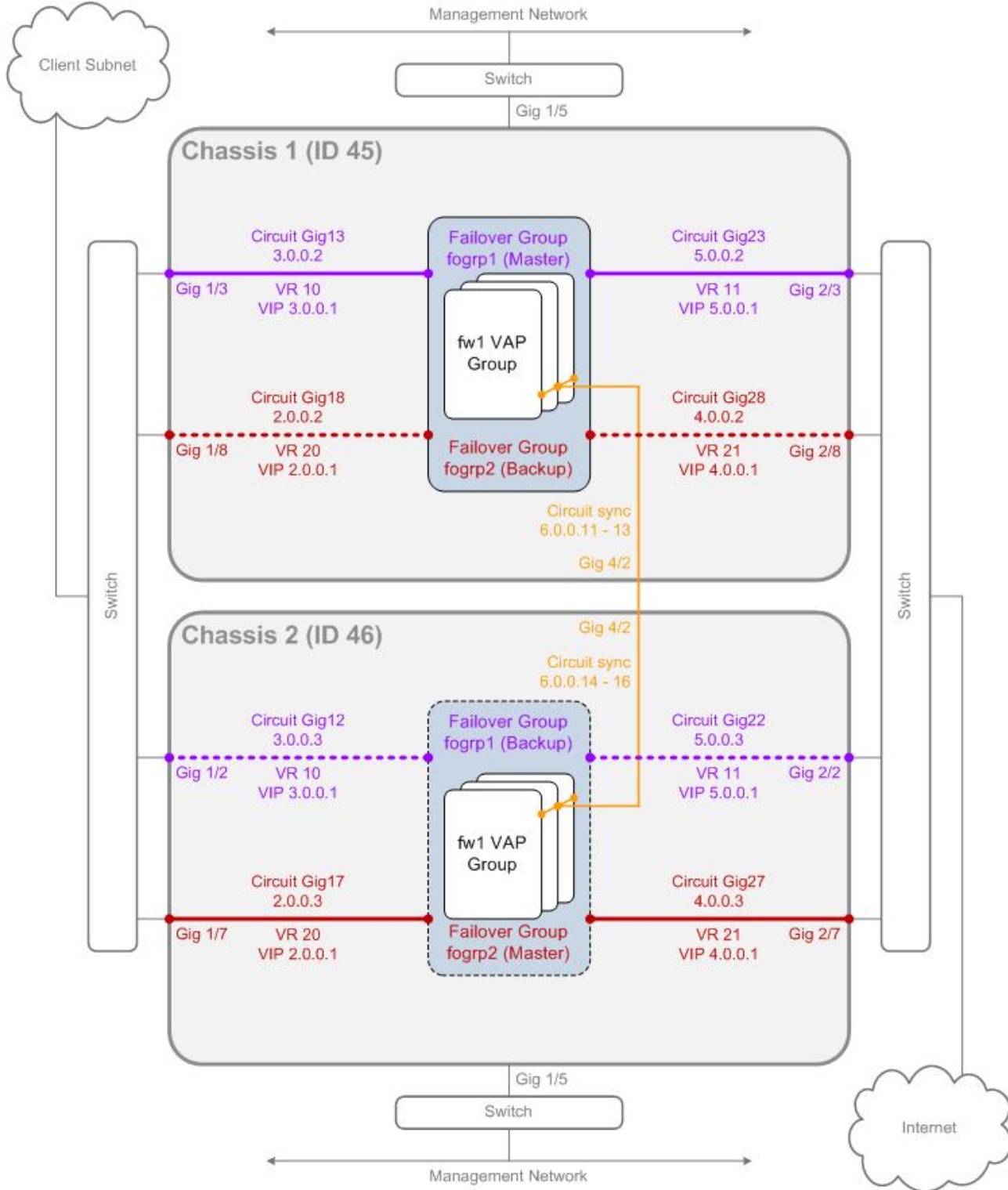
Active-Active Configuration

This section describes how to configure the two chassis for Active-Active VRRP Dual-box High Availability operation. See:

- [System Diagram \(Active-Active\)](#) on page 41
- [Configuring Chassis 1](#) on page 42
- [Configuring Chassis 2](#) on page 56

System Diagram (Active-Active)

This diagram illustrates the goal of the configuration steps in this chapter.



1.0 Configuring Chassis 1

On Chassis 1, perform these tasks:

- [Configuring System-wide Parameters \(Chassis 1\)](#)
- [Configuring Failover Group 1 \(Chassis 1\)](#)
- [Configuring Failover Group 2 \(Chassis 1\)](#)

1.1 Configuring System-wide Parameters (Chassis 1)

1.1.1 Local System Identifier

Configure the local `system-identifier` on Chassis 1.

NOTE: When configuring multiple chassis for high availability, a unique system ID must be assigned to each chassis. If both chassis are configured with the same ID, you run the risk of having identical MAC addresses on any given circuit. Such a configuration is **not** supported or recommended.

If your X-Series Platforms do not have unique system IDs assigned, use the following command to define a system ID. The valid range is from 1-255.

```
CBS# configure system-identifier 45
```

NOTE: After you configure the `system-identifier` parameter, you must use the `reload all` command to activate the identifier.

1.1.2 Remote System Identifier

NOTE: Crossbeam recommends that you connect the two chassis using the guidelines described in [Chassis Interconnection](#) on page 18, and then use the `configure remote-box` command on both chassis to specify ports on the remote chassis.

Configure the remote system ID and IP address using the `configure remote-box` command.

NOTE: The `configure remote-box` command requires that you have interconnected CPMs on the two chassis. Crossbeam recommends that you specify the following IP addresses. See [Chassis Interconnection](#) on page 18

- For the High Availability port, specify the **internal** IP address (1.1.46.20) associated with the remote Primary CPM (obtained by running `show-internal-ip` on the remote chassis).
- For the management ports, specify the **external** IP address(es) associated with the port(s).

```
CBS# configure remote-box 46 1.1.46.20 192.168.50.46 192.168.51.56
CBS(conf-remote-box) # end
```

NOTE: The example `configure remote-box` command specifies only the IP addresses of the management 1 and 2 interfaces and the internal IP address for the primary CPM on chassis 2. Crossbeam recommends that you connect the management interfaces of the other CPM on Chassis 2, and add the IP addresses for those interfaces to the `configure remote-box` command.

1.1.3 Configuring the Synchronization Circuit

Configure a synchronization circuit between VAP Group fw1 on Chassis 1 and fw1 on Chassis 2 so that the two VAP Groups act as one Check Point Cluster with 6 members.

NOTE: This step must be performed **after** you configure the system ID, because the system ID affects the MAC selection and configuration of every circuit that gets created.

Enter these commands:

```
CBS# configure circuit sync
CBS (conf-cct) # device-name sync
CBS (conf-cct) # link-state-resistant
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 6.0.0.11/24 increment-per-vap 6.0.0.13
CBS (conf-cct-vapgroup) # end
CBS#
CBS# configure interface gigabitethernet 4/2
CBS (conf-intf-gig) # logical sync
CBS (intf-gig-logical) # circuit sync
CBS (intf-gig-log-cct) # end
CBS#
```

1.1.4 Configure the Traffic Circuits

Configure the two circuits that convey traffic to and from the fw1 VAP group.

```
CBS# configure circuit Gig13
CBS (conf-cct) # device-name Gig13
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 3.0.0.2/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS# configure circuit Gig23
CBS (conf-cct) # device-name Gig23
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 5.0.0.2/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS# configure circuit Gig18
CBS (conf-cct) # device-name Gig18
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 2.0.0.2/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS# configure circuit Gig28
CBS (conf-cct) # device-name Gig28
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 4.0.0.2/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS#
```

1.1.5 Configure the Traffic Interfaces

Configure the interfaces through which traffic flows to and from the fw1 VAP group.

```
CBS# configure interface gigabitethernet 1/3
CBS(conf-intf-gig)# logical Gig13
CBS(intf-gig-logical)# circuit Gig13
CBS(intf-gig-log-cct)# end
CBS#
CBS# configure interface gigabitethernet 2/3
CBS(conf-intf-gig)# logical Gig23
CBS(intf-gig-logical)# circuit Gig23
CBS(intf-gig-log-cct)# end
CBS#
CBS# configure interface gigabitethernet 1/8
CBS(conf-intf-gig)# logical Gig18
CBS(intf-gig-logical)# circuit Gig18
CBS(intf-gig-log-cct)# end
CBS#
CBS# configure interface gigabitethernet 2/8
CBS(conf-intf-gig)# logical Gig28
CBS(intf-gig-logical)# circuit Gig28
CBS(intf-gig-log-cct)# end
CBS#
```

1.2 Configuring Failover Group 1 (Chassis 1)

1.2.1 VRRP Failover Group

Create the failover group by assigning it a name (`fogrp1`) and a failover group ID. The failover group ID is different than the system identifier, configured earlier. The ID must be unique on this chassis, and must be the same on its counterpart failover group on the remote chassis (Chassis 2).

The `fogrp1` group acts as the master group on Chassis 1. The counterpart failover group on Chassis 2 is also called `fogrp1` and has the same group ID (1).

```
CBS# configure vrrp failover-group fogrp1 failover-group-id 1
CBS(conf-vrrp-group)#
```

1.2.2 VRRP Priority

For proper operation, the VRRP `priority` value of the two associated failover groups must be different on Chassis 1 and Chassis 2; during normal operations, the failover group with the higher priority is the master. Certain events, such as an interface failure or a change in VAP group member count, can be configured to decrement the VRRP priority of a failover group. Failover occurs when the VRRP `priority` value of the master failover group drops below the priority of the backup failover group on the other chassis. VRRP `priority` values range from 1 to 255, and the default is 100.

```
CBS(conf-vrrp-group)# priority 250
CBS(conf-vrrp-group)# exit
```

1.2.3 Virtual Router on each Traffic Circuit

Create a virtual router on each traffic circuit that is attached to the fw1 VAP group. A virtual router is assigned a virtual IP addresses that is used to configure VRRP and, optionally, next hop health check. This section describes the configuration of two virtual routers, one for each of the two circuits (Gig18 and Gig28) that are associated with the fw1 vap-group.

Configuring the virtual-router for the Gig13 circuit

1. To create the virtual router for the first circuit, enter this command.

```
CBS(conf-vrrp-group) # virtual-router vrrp-id 10 circuit Gig13
CBS(conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS(conf-vrrp-failover-vr) # priority-delta 2
CBS(conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's `priority` value is decremented by the `priority-delta` value to a new `priority` value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the `priority` value on Chassis 1 decrements by to from 250 to 248. The new value is compared to the priority value of the associated failover group on Chassis 2, which is 249. Based on the comparison, a failover event occurs and the failover group on Chassis 2 becomes master.

The `priority-delta` value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS(conf-vrrp-failover-vr) # mac-usage vrrp-mac
CBS(conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS(conf-vrrp-failover-vr) # vap-group fw1
CBS(conf-vrrp-vr-vapgroup) #
```

NOTE: Before you map the virtual router to the VAP group, the circuit must have been mapped to the VAP group. Mapping the VAP group to the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS(conf-vrrp-vr-vapgroup) # virtual-ip 3.0.0.1/24
CBS(conf-vrrp-vr-vapgroup) # end
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

Configuring the virtual-router for the Gig23 circuit

1. To create the virtual router for the second circuit, enter this command.

```
CBS# configure vrrp failover-group fogrpl failover-group-id 1  
CBS (conf-vrrp-group) # virtual-router vrrp-id 11 circuit Gig23  
CBS (conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS (conf-vrrp-failover-vr) # priority-delta 2  
CBS (conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's priority value is decremented by the `priority-delta` value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the `priority` value on Chassis 1 becomes 248, which is less than the `priority` value of the associated failover group on Chassis 2, so the failover group on Chassis 2 becomes the master. The `priority-delta` value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS (conf-vrrp-failover-vr) # mac-usage vrrp-mac
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS (conf-vrrp-failover-vr) # vap-group fw1  
CBS (conf-vrrp-vr-vapgroup) #
```

NOTE: The circuit must already be mapped to the VAP group.

Specifying the VAP group of the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS (conf-vrrp-vr-vapgroup) # virtual-ip 5.0.0.1/24  
CBS (conf-vrrp-vr-vapgroup) # end  
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

1.2.1 Enable VRRP on the VAP Group

To configure the fw1 VAP group for failover:

1. Enable VRRP on the fw1 VAP group.

```
CBS# configure vrrp vap-group fw1
CBS(conf-vrrp-vap-group) #
```

2. Assign the VRRP enabled fw1 VAP group to a failover group list (required).

```
CBS(conf-vrrp-vap-group) # failover-group-list fogrpl fogrp2
CBS(conf-vrrp-vap-group) #
```

3. Optionally, set the hold down timer.

Configure the `hold-down-timer` to 120, which forces the VAP group to wait for two minutes while the application fully boots. This delay prevents the failover group from becoming VRRP master before the application is fully active.

```
CBS(conf-vrrp-vap-group) # hold-down-timer 120
CBS(conf-vrrp-vap-group) #
```

4. Optionally, set the active VAP threshold and return to the main CLI context.

The `active-vap-threshold` monitors the VAPs in the VAP group. If the number of active VAPs drops below the threshold, the group's priority value is decremented by the `priority-delta`. Failover occurs when the `priority-delta` decrements the priority value of the master failover group below the priority value of the backup group.

```
CBS(conf-vrrp vap-group) # active-vap-threshold 3
CBS(conf-vrrp vap-group) # end
CBS#
```

5. Set the `priority-delta` value for the VAP group (optional).

Assign a `priority-delta` to the VAP group. VRRP decrements the priority of the failover group whenever the number of active VAPs falls below the `active-vap-threshold`.

The `priority-delta` value can be any number between 1 and 255 and the default value is 1. When the VAP returns to the Active state, the `priority-delta` value is added back to the priority value.

```
CBS(conf-vrrp-vap-group) # priority-delta 2
```

1.3 Optionally Configuring OSPF

If your network is configured to use the Open Shortest Path First (OSPF) protocol, you can modify the OSPF routes to reflect the VRRP state.

NOTE: To configure OSPF, you must first install the Crossbeam Routing Software (RSW).

When a failover occurs from one failover group to another, you want traffic to be rerouted from the failed group to the one that is now active. To ensure that this happens, you can increase the `ospf-cost-increment` value associated with the circuit on the first failover group. The new value is propagated to all local routers, increasing the OSPF cost of the circuit so that it is no longer part of the preferred route. When the original failover group resumes master status, the OSPF cost is readjusted to the originally configured value.

NOTE: Configure the `ospf-cost-increment` only on the master failover group.

To include OSPF cost in the configuration, perform these steps:

1. Configure these parameters on the master failover group (`fogrp1`):

```
CBS# configure vrrp failover-group fogrp1
CBS (conf-vrrp-group) # ospf-cost-increment circuit Gig18 5
CBS (conf-vrrp-group) # ospf-cost-increment circuit Gig28 5
```

2. On the VAP group that is associated with the master failover group, start the OSPF routing protocol.

```
CBS# configure routing-protocol ospf vap-group fw1 start
```

1.4 Preemption

Typically, after a failover has occurred from one failover group to another, you want the failover group that is now master to remain in that role, even after the problem that caused the failover has been resolved.

By default, preemption is turned off, and Crossbeam recommends that you do not configure preemption for failover groups.

However, if you want the original failover group to resume the role of master, you can turn preemption on using this command.

```
CBS (conf-vrrp-group) # preemption
```

1.5 Management Circuit

If you intend to run Check Point software on the X-Series chassis, do not configure the X-Series chassis management circuits as part of any failover group. This configuration is poor design and prevents access by the Check Point management station to the management circuit on the chassis on which the backup failover groups reside .

1.6 Configuring Failover Group 2 (Chassis 1)

1.6.1 VRRP Failover Group

Create the failover group by assigning it a name (`fogrp2`) and a failover group ID. The failover group ID is different than the system identifier, configured earlier. The ID must be unique on this chassis, and must be the same on its counterpart failover group on the remote chassis (Chassis 2).

The `fogrp2` group on Chassis 1 acts as the backup group to the master `fogrp2` group on Chassis 2. Both groups have the same group ID (2). The two groups have different priority values.

```
CBS# configure vrrp failover-group fogrp2 failover-group-id 2
CBS (conf-vrrp-group) #
```

1.6.2 VRRP Priority

For proper operation, the VRRP priority value of the two associated failover groups must be different on Chassis 1 and Chassis 2; during normal operations, the failover group with the higher priority is the master. Certain events such as an interface failure or a change in VAP group member count can be configured to decrement the VRRP priority of the failover group. Failover occurs when the VRRP priority value of one failover group drops below the priority of the failover group on the other chassis. VRRP priority values range from 1 to 255, and the default is 100.

```
CBS (conf-vrrp-group) # priority 249
```

1.6.3 Virtual Router on each Traffic Circuit

Create a virtual router on each traffic circuit that is attached to the `fw1` VAP group. A virtual router is assigned a virtual IP addresses that is used to configure VRRP and, optionally, next hop health check. This section describes the configuration of two virtual routers, one for each of the two circuits (`Gig18` and `Gig28`) that are associated with the `fw1` VAP group.

Configuring the virtual-router for the Gig18 circuit

1. To create the virtual router for the first circuit, enter this command.

```
CBS (conf-vrrp-group) # virtual-router vrrp-id 20 circuit Gig18
CBS (conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a priority-delta value to the virtual router.

```
CBS (conf-vrrp-failover-vr) # priority-delta 2  
CBS (conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's priority value is decremented by the priority-delta value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the priority value on Chassis 2 becomes 248, which is less than the priority value of the associated failover group on Chassis 1, so the failover group on Chassis 1 becomes the master. The priority-delta value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS (conf-vrrp-failover-vr) # mac-usage vrrp-mac  
CBS (conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS (conf-vrrp-failover-vr) # vap-group fw1  
CBS (conf-vrrp-vr-vapgroup) #
```

NOTE: Before you map the virtual router to the VAP group, the circuit must have been mapped to the VAP group. Mapping the VAP group to the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS (conf-vrrp-vr-vapgroup) # virtual-ip 2.0.0.1/24  
CBS (conf-vrrp-vr-vapgroup) # end  
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

Configuring the virtual-router for the Gig28 circuit

1. To create the virtual router for the second circuit, enter this command.

```
CBS# configure vrrp failover-group fogrp2 failover-group-id 2  
CBS (conf-vrrp-group) # virtual-router vrrp-id 21 circuit Gig28  
CBS (conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a priority-delta value to the virtual router.

```
CBS (conf-vrrp-failover-vr) # priority-delta 2  
CBS (conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's priority value is decremented by the `priority-delta` value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the priority value on Chassis 1 becomes 248, which is less than the priority value of the

associated failover group on Chassis 2, so the failover group on Chassis 2 becomes the master. The `priority-delta` value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS(conf-vrrp-failover-vr) # mac-usage vrrp-mac
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS(conf-vrrp-failover-vr) # vap-group fw1
CBS(conf-vrrp-vr-vapgroup) #
```

NOTE: The circuit must already be mapped to the VAP group.

Specifying the VAP group of the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS(conf-vrrp-vr-vapgroup) # virtual-ip 4.0.0.1/24
CBS(conf-vrrp-vr-vapgroup) # end
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

1.6.4 Enable VRRP on the VAP Group

VRRP monitors the `fw1` VAP group for failure of individual VAPs. By setting the `active-vap-threshold` and the `priority-delta`, individual VAP failures can decrement VRRP priority and cause a comparison with the VRRP priority on the remote chassis. Failover occurs when the `priority-delta` value decrements the priority value of the master failover group below the priority value of the associated failover group on the remote chassis. In our configuration, the priority value for the master failover group is 250 and the priority value for the backup group is 249. A `priority-delta` of 2 is used for each of the VAP groups.

To configure the `fw1` VAP group for failover:

1. Enable VRRP on the `fw1` VAP group.

```
CBS# configure vrrp vap-group fw1
CBS(conf-vrrp-vap-group) #
```

2. Assign the VRRP enabled `fw1` VAP group to a failover group list (required).

```
CBS(conf-vrrp-vap-group) # failover-group-list fogrp1 fogrp2
CBS(conf-vrrp-vap-group) #
```

3. Optionally, set the hold down timer.

Configure the `hold-down-timer` to 120, which forces the VAP group to wait for two minutes while the application fully boots. This wait prevents the failover group from becoming VRRP master before the application is fully active.

```
CBS(conf-vrrp-vap-group) # hold-down-timer 120
CBS(conf-vrrp-vap-group) #
```

4. Optionally, set the active VAP threshold and return to the main CLI context.

The `active-vap-threshold` monitors the number of active VAPs in the VAP group. If the number of active VAPs drops below the threshold, the failover group's priority value is decremented by the `priority-delta` (defined in Step 5) and a comparison is done between the priorities of the failover groups on the two chassis. Failover occurs when the `priority-delta` decrements the priority value of the master failover group below the priority value of the backup group.

```
CBS (conf-vrrp vap-group) # active-vap-threshold 3
CBS (conf-vrrp vap-group) # end
CBS#
```

5. Set the `priority-delta` value for the VAP group (optional).

Assign a `priority-delta` to the VAP group. VRRP decrements the priority of the failover group whenever the number of active VAPs falls below the `active-vap-threshold`.

The `priority-delta` value can be any number between 1 and 255 and the default value is 1. When the VAP returns to the Active state, the `priority-delta` value is added back to the `priority` value.

```
CBS (conf-vrrp-vap-group) # priority-delta 2
CBS (conf-vrrp-vap-group) # exit
```

NOTE: Do not configure any OSPF cost increments for the circuits associated with `fogrp2` group on chassis 1. OSPF is configured only for master failover groups.

1.7 Preemption

Typically, after a failover has occurred from one failover group to another, you want the failover group that is now master to remain in that role, even after the problem that caused the failover has been resolved.

By default, preemption is turned off, and Crossbeam recommends that you do not configure preemption for failover groups.

However, if you want the original failover group to resume the role of master, you can turn preemption on using this command.

```
CBS (conf-vrrp-group) # preemption
```

1.8 Management Circuit

If you intend to run Check Point software on the X-Series chassis, do not configure the X-Series chassis management circuits as part of any failover group. This configuration is poor design and prevents access by the Check Point management station to the management circuit on the chassis on which the backup failover groups reside .

1.9 Verifying Your Configuration

This section contains the output of several commands that show the configured status of Chassis 1. To check your progress throughout the configuration process, open a second CLI window, log in to the CPM and enter one of the commands.

Output of show running-config on Chassis 1

```
CBS# show running-config
#
remote-box 46 1.1.46.20 192.168.50.46 192.168.51.56
#
vap-group fw1 xslinux_v5
vap-count 3
  max-load-count 3
  ap-list ap1 ap2 ap3 ap4 ap5 ap6 ap7 ap8 ap9 ap10
  load-balance-vap-list 1 2 3 4 5 6 7 8 9 10
  ip-flow-rule loadbalance1
    action load-balance
    activate
#
circuit Gig13 circuit-id 1025
  device-name Gig13
  vap-group fw1
    ip 3.0.0.2/24 3.0.0.255
circuit Gig23 circuit-id 1026
  device-name Gig23
  vap-group fw1
    ip 5.0.0.2/24 5.0.0.255
circuit Gig18 circuit-id 1027
  device-name Gig18
  vap-group fw1
    ip 2.0.0.2/24 2.0.0.255
circuit Gig28 circuit-id 1028
  device-name Gig28
  vap-group fw1
    ip 4.0.0.2/24 4.0.0.255
circuit sync circuit-id 1029
  device-name sync
  link-state-resistant
  vap-group fw1
    ip 6.0.0.11/24 6.0.0.255 increment-per-vap 6.0.0.13
#
#
interface gigabitethernet 1/3
  logical Gig13
  circuit Gig13
interface gigabitethernet 2/3
  logical Gig23
  circuit Gig23
interface gigabitethernet 1/8
  logical Gig18
  circuit Gig18
interface gigabitethernet 2/8
  logical Gig28
  circuit Gig28
#
```

Chapter 3: Active-Active VRRP Dual-Box High Availability Configuration

```
#
vrrp failover-group fogrp1 failover-group-id 1
  priority 250
  virtual-router vrrp-id 10 circuit Gig13
    priority-delta 2
  vap-group fw1
    virtual-ip 3.0.0.1/24 3.0.0.255
  virtual-router vrrp-id 11 circuit Gig23
    priority-delta 2
  vap-group fw1
    virtual-ip 5.0.0.1/24 5.0.0.255
vrrp failover-group fogrp2 failover-group-id 2
  priority 249
  virtual-router vrrp-id 20 circuit Gig18
    priority-delta 2
  vap-group fw1
    virtual-ip 2.0.0.1/24 2.0.0.255
  virtual-router vrrp-id 21 circuit Gig28
    priority-delta 2
  vap-group fw1
    virtual-ip 4.0.0.1/24 4.0.1.255
#
vrrp vap-group fw1
  failover-group-list fogrp1 fogrp2
  hold-down-timer 120
  priority-delta 2
#
management gigabitethernet 13/1
  ip-addr 192.168.50.45/24 192.168.50.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 13/2
  ip-addr 192.168.51.55/24 192.168.51.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 14/1
  ip-addr 192.168.50.65/24 192.168.50.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 14/2
  ip-addr 192.168.51.75/24 192.168.51.255
  enable
  access-list 1 input
  access-list 2 output
```

Output of show vrrp on Chassis 1

```
CBS# show vrrp
Priority is Actual/Configured
FG-ID Priority Status Preempt Master Sys ID Master Priority
1 250/250 Master off 45 250
2 249/249 Backup off 46 250
(1 row)
```

Output of show vrrp detail-status on Chassis 1

```
CBS# show vrrp detail-status
FG_ID  Status  Priority  Delta  Type  Component
  1  Master  250/250    2    vr  Gig18/10/5
  1  Master  250/250    2    vr  Gig28/10/5
  1  Master  250/250    2    vg  fw1
  2  Backup  249/249    2    vr  Gig18/10/0
  2  Backup  249/249    2    vr  Gig28/10/0
  2  Backup  249/249    2    vg  fw1
```

NOTE: The Component column shows 5 as the last digit only if you configured the OSPF cost increment as described in [Optionally Configuring OSPF](#) on page 48. If you did not configure the OSPF cost increment, these values would be 0 (zero).

Output of show remote-box on Chassis 1

```
CBS# show remote-box
Local System ID: 45

Remote System ID: 46
Remote IP      Local Intf  Local IP      Status  Time In State  Link Qual
192.168.50.46  14/1       192.168.50.45 Active  9 days, 03:10  100
192.168.51.56  14/2       192.168.51.55 Active  9 days, 02:07  100
1.1.46.20      HA port    1.1.45.20     Active  9 days, 02:07  100
(3 rows)
```

2.0 Configuring Chassis 2

On Chassis 2, perform these tasks:

- [Configuring System-wide Parameters \(Chassis 2\)](#)
- [Configuring Failover Group 1 \(Chassis 2\)](#)
- [Configuring Failover Group 2 \(Chassis 2\)](#)

2.1 Configuring System-wide Parameters (Chassis 2)

2.1.1 Local System Identifier

Configure the local `system-identifier` on Chassis 2.

NOTE: When configuring multiple chassis for high availability, a unique system ID must be assigned to each chassis. If both chassis are configured with the same ID, you run the risk of having identical MAC addresses on any given circuit. This configuration is **not** supported or recommended.

If your X-Series Platforms do not have unique system IDs assigned, use the following command to define a system ID. The valid range is from 1-255.

```
CBS# configure system-identifier 46
```

NOTE: After you configure the `system-identifier` parameter, you must use the `reload all` command to activate the identifier.

2.1.2 Remote System Identifier

NOTE: Crossbeam recommends that you connect the two chassis using the guidelines described in [Chassis Interconnection](#) on page 18, and then use the `configure remote-box` command on both chassis to configure ports on the remote chassis.

Configure the remote system ID and IP address using the `configure remote-box` command.

NOTE: The `configure remote-box` command requires that you have interconnected CPMs on the two chassis. Crossbeam recommends that you specify the following IP addresses.

- For the High Availability port, specify the **internal** IP address (1.1.46.20) associated with the remote Primary CPM (obtained by running `show-internal-ip` on the remote chassis).
- For the management ports, specify the **external** IP address(es) associated with the port(s).

```
CBS# configure remote-box 45 1.1.45.20 192.168.50.45 192.168.51.55  
CBS(conf-remote-box) # end
```

NOTE: The example `configure remote-box` command specifies only the IP addresses of the management 1 and 2 interfaces and the internal IP address for the primary CPM on chassis 1. Crossbeam recommends that you connect the management interfaces of the other CPM on Chassis 1, and add the IP addresses for those interfaces to the `configure remote-box` command.

2.1.3 Configuring the Synchronization Circuit

Configure a synchronization circuit between VAP Group fw1 on Chassis 2 and fw1 on Chassis 1 so that the two VAP Groups act as one Check Point Cluster with 6 members.

NOTE: This step must be performed **after** you configure the system ID, because the system ID affects the MAC selection and configuration of every circuit that gets created.

Enter these commands:

```
CBS# configure circuit sync
CBS (conf-cct) # device-name sync
CBS (conf-cct) # link-state-resistant
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 6.0.0.14/24 increment-per-vap 6.0.0.16
CBS (conf-cct-vapgroup) # end
CBS#
CBS# configure interface gigabitethernet 4/2
CBS (conf-intf-gig) # logical sync
CBS (intf-gig-logical) # circuit sync
CBS (intf-gig-log-cct) # end
CBS#
```

2.1.4 Configure the Traffic Circuits

Configure the two circuits that convey traffic to and from the fw1 VAP group.

```
CBS# configure circuit Gig12
CBS (conf-cct) # device-name Gig12
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 3.0.0.3/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS# configure circuit Gig22
CBS (conf-cct) # device-name Gig22
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 5.0.0.3/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS# configure circuit Gig17
CBS (conf-cct) # device-name Gig17
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 2.0.0.3/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS# configure circuit Gig27
CBS (conf-cct) # device-name Gig27
CBS (conf-cct) # vap-group fw1
CBS (conf-cct-vapgroup) # ip 4.0.0.3/24
CBS (conf-cct-vapgroup-ip) # enable
CBS (conf-cct-vapgroup-ip) # end
CBS#
```

2.1.5 Configure the Traffic Interfaces

Configure the interfaces through which traffic flows to and from the fw1 VAP group.

```
CBS# configure interface gigabitethernet 1/7
CBS(conf-intf-gig)# logical Gig17
CBS(intf-gig-logical)# circuit Gig17
CBS(intf-gig-log-cct)# end
CBS#
CBS# configure interface gigabitethernet 2/7
CBS(conf-intf-gig)# logical Gig27
CBS(intf-gig-logical)# circuit Gig27
CBS(intf-gig-log-cct)# end
CBS#
```

2.2 Configuring Failover Group 1 (Chassis 2)

2.2.1 VRRP Failover Group

Create the failover group by assigning it a name (`fogrp1`) and a failover group ID. The failover group ID is different than the system identifier, configured earlier. The ID must be unique on this chassis, and must be the same on its counterpart failover group on the remote chassis (Chassis 1).

The `fogrp1` group on Chassis 2 acts as the backup group to the master `fogrp1` group on Chassis 1. Both groups have the same group ID (1). The two groups have different `priority` values.

```
CBS# configure vrrp failover-group fogrp1 failover-group-id 1
CBS(conf-vrrp-group)#
```

2.2.2 VRRP Priority

For proper operation, the VRRP `priority` value of the two associated failover groups must be different on Chassis 1 and Chassis 2; during normal operations, the failover group with the higher priority is the master. Certain events such as an interface failure or a change in VAP group member count can be configured to decrement the VRRP priority of the failover group. Failover occurs when the VRRP `priority` value of one failover group drops below the priority of the failover group on the other chassis. VRRP `priority` values range from 1 to 255, and the default is 100.

```
CBS(conf-vrrp-group)# priority 249
CBS(conf-vrrp-group)# exit
```

2.2.3 Virtual Router on each Traffic Circuit

Create a virtual router on each traffic circuit that is attached to the fw1 VAP group. A virtual router is assigned a virtual IP addresses that is used to configure VRRP and, optionally, next hop health check. This section describes the configuration of two virtual routers, one for each of the two circuits (`Gig17` and `Gig27`) that are associated with the fw1 VAP group.

Configuring the virtual-router for the Gig12 circuit

1. To create the virtual router for the first circuit, enter this command.

```
CBS(conf-vrrp-group) # virtual-router vrrp-id 10 circuit Gig12
CBS(conf-vrrp-failover-vr) #
```

NOTE: NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS(conf-vrrp-failover-vr) # priority-delta 2
CBS(conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's `priority` value is decremented by the `priority-delta` value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the priority value on Chassis 1 becomes 248, which is less than the `priority` value of the associated failover group on Chassis 2, so the failover group on Chassis 2 becomes the master. The `priority-delta` value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS(conf-vrrp-failover-vr) # mac-usage vrrp-mac
CBS(conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS(conf-vrrp-failover-vr) # vap-group fw1
CBS(conf-vrrp-vr-vapgroup) #
```

NOTE: Before you map the virtual router to the VAP group, the circuit must have been mapped to the VAP group. Mapping the VAP group to the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS(conf-vrrp-vr-vapgroup) # virtual-ip 3.0.0.1/24
CBS(conf-vrrp-vr-vapgroup) # end
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

Configuring the virtual-router for the Gig22 circuit

1. To create the virtual router for the second circuit, enter this command.

```
CBS# configure vrrp failover-group fogrpl failover-group-id 1  
CBS (conf-vrrp-group) # virtual-router vrrp-id 11 circuit Gig22  
CBS (conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS (conf-vrrp-failover-vr) # priority-delta 2  
CBS (conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's `priority` value is decremented by the `priority-delta` value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the `priority` value on Chassis 1 becomes 248, which is less than the `priority` value of the associated failover group on Chassis 2, so the failover group on Chassis 2 becomes the master. The `priority-delta` value is added back to the priority when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS (conf-vrrp-failover-vr) # mac-usage vrrp-mac  
CBS (conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS (conf-vrrp-failover-vr) # vap-group fw1  
CBS (conf-vrrp-vr-vapgroup) #
```

NOTE: The circuit must already be mapped to the VAP group.

Specifying the VAP group of the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS (conf-vrrp-vr-vapgroup) # virtual-ip 5.0.0.1/24  
CBS (conf-vrrp-vr-vapgroup) # end  
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2.2.4 Enable VRRP on the VAP Group

VRRP monitors the fw1 VAP group for failure of individual VAPs. By setting the `active-vap-threshold` and the `priority-delta`, individual VAP failures can decrement VRRP `priority` and cause a failover. Failover occurs when the `priority-delta` value decrements the `priority` value of the master failover group below the `priority` value of the associated failover group on the remote chassis. In our configuration, the `priority` value for the master failover group is 250 and the `priority` value for the backup group is 249. A `priority-delta` of 2 is used for each of the VAP groups.

To configure the fw1 VAP group for failover:

1. Enable VRRP on the fw1 VAP group.

```
CBS# configure vrrp vap-group fw1
CBS(conf-vrrp-vap-group) #
```

2. Assign the VRRP enabled fw1 VAP group to a failover group list (required).

```
CBS(conf-vrrp-vap-group) # failover-group-list fogrp1 fogrp2
```

3. Optionally, set the hold down timer.

Configure the `hold-down-timer` to 120, which forces the VAP group to wait for two minutes while the application fully boots. This wait prevents the failover group from becoming VRRP master before the application is fully active.

```
CBS(conf-vrrp-vap-group) # hold-down-timer 120
```

4. Optionally, set the active VAP threshold and return to the main CLI context.

The `active-vap-threshold` monitors the VAPs in the VAP group. If the number of active VAPs drops below the threshold, the group's `priority` value is decremented by the `priority-delta`. Failover occurs when the `priority-delta` decrements the `priority` value of the master failover group below the `priority` value of the backup group.

```
CBS(conf-vrrp vap-group) # active-vap-threshold 3
CBS(conf-vrrp vap-group) # end
CBS#
```

5. Set the `priority-delta` value for the VAP group (optional).

Assign a `priority-delta` to the VAP group. VRRP decrements the `priority` of the failover group whenever the number of active VAPs falls below the `active-vap-threshold`.

The `priority-delta` value can be any number between 1 and 255 and the default value is 1. When the VAP returns to the Active state, the `priority-delta` value is added back to the `priority` value.

```
CBS(conf-vrrp-vap-group) # priority-delta 2
CBS(conf-vrrp-vap-group) # exit
```

NOTE: Do not configure any OSPF cost increments for the circuits associated with `fogrp1` group on chassis 2. OSPF is configured only for master failover groups.

2.3 Optionally Configuring OSPF

If your network is configured to use the Open Shortest Path First (OSPF) protocol, you can incorporate OSPF into your VRRP configuration.

NOTE: To configure OSPF, you must first install the Crossbeam Routing Software (RSW).

When a failover occurs from one failover group to another, you want traffic to be rerouted from the failed group to the one that is now active. To ensure that this happens, you can increase the `ospf-cost-increment` value associated with the circuit on the first failover group. The new value is propagated to all local routers, increasing the OSPF cost of the circuit so that it is no longer part of the preferred route. When the original failover group resumes master status, the OSPF cost is readjusted to the originally configured value.

NOTE: Configure the `ospf-cost-increment` only on the master failover group.

To include OSPF cost in the configuration, perform these steps:

1. Configure these parameters on the master failover group (`fogrpl`):

```
CBS# configure vrrp failover-group fogrpl
CBS (conf-vrrp-group) # ospf-cost-increment circuit Gig18 5
CBS (conf-vrrp-group) # ospf-cost-increment circuit Gig28 5
CBS (conf-vrrp-group) # end
CBS#
```

2. On the VAP group that is associated with the master failover group, start the ospf routing protocol.

```
CBS# configure routing-protocol ospf vap-group fw1 start
```

2.4 Preemption

Typically, after a failover has occurred from one failover group to another, you want the failover group that is now master to remain in that role, even after the problem that caused the failover has been resolved.

By default, preemption is turned off, and Crossbeam recommends that you do not configure preemption for failover groups.

However, if you want the original failover group to resume the role of master, you can turn preemption on using this command.

```
CBS (conf-vrrp-group) # preemption
```

2.5 Management Circuit

If you intend to run Check Point software on the X-Series chassis, do not configure the X-Series chassis management circuits as part of any failover group. This configuration is poor design and prevents access by the Check Point management station to the management circuit on the chassis on which the backup failover groups reside .

2.6 Configuring Failover Group 2 (Chassis 2)

2.6.1 VRRP Failover Group

Create the failover group by assigning it a name (`fogrp2`) and a failover group ID. The failover group ID is different than the system identifier, configured earlier. The ID must be unique on this chassis, and must be the same on its counterpart failover group on the remote chassis (Chassis 1).

The `fogrp2` group acts as the master group on Chassis 2. The counterpart failover group on Chassis 1 is also called `fogrp2` and has the same group ID (2). The two groups have different `priority` values.

```
CBS# configure vrrp failover-group fogrp2 failover-group-id 2
CBS(conf-vrrp-group) #
```

2.6.2 VRRP Priority

For proper operation, the VRRP `priority` value of the two associated failover groups must be different on Chassis 1 and Chassis 2; during normal operations, the failover group with the higher priority is the master. Certain events such as an interface failure or a change in VAP group member count can be configured to decrement the VRRP `priority` of the failover group. Failover occurs when the VRRP `priority` value of one failover group drops below the `priority` of the failover group on the other chassis. VRRP priority values range from 1 to 255, and the default is 100.

```
CBS(conf-vrrp-group) # priority 250
CBS(conf-vrrp-group) #
```

2.6.3 Virtual Router on each Traffic Circuit

Create a virtual router on each traffic circuit that is attached to the `fw1` VAP group. A virtual router is assigned a virtual IP addresses that is used to configure VRRP and, optionally, next hop health check. This section describes the configuration of two virtual routers, one for each of the two circuits (`Gig17` and `Gig27`) that are associated with the `fw1` vap-group.

Configuring the virtual-router for the Gig17 circuit

1. To create the virtual router for the first circuit, enter this command.

```
CBS(conf-vrrp-group) # virtual-router vrrp-id 20 circuit Gig17  
CBS(conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS(conf-vrrp-failover-vr) # priority-delta 2  
CBS(conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's `priority` value is decremented by the `priority-delta` value (2) to a new priority value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the `priority` value on Chassis 2 becomes 248, which is less than the `priority` value of the associated failover group on Chassis 1, so the failover group on Chassis 1 becomes the master. The `priority-delta` value is added back to the `priority` when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS(conf-vrrp-failover-vr) # mac-usage vrrp-mac  
CBS(conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS(conf-vrrp-failover-vr) # vap-group fw1  
CBS(conf-vrrp-vr-vapgroup) #
```

NOTE: Before you map the virtual router to the VAP group, the circuit must have been mapped to the VAP group. Mapping the VAP group to the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS(conf-vrrp-vr-vapgroup) # virtual-ip 2.0.0.1/24  
CBS(conf-vrrp-vr-vapgroup) # end
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

Configuring the virtual-router for the Gig27 circuit

1. To create the virtual router for the second circuit, enter this command.

```
CBS(conf-vrrp-group) # virtual-router vrrp-id 21 circuit Gig27
CBS(conf-vrrp-failover-vr) #
```

NOTE: Any circuit that is defined as part of a virtual router is automatically monitored for failure, and, when one occurs, the failover group's priority is decremented by the `priority-delta` value.

2. Assign a `priority-delta` value to the virtual router.

```
CBS(conf-vrrp-failover-vr) # priority-delta 2
CBS(conf-vrrp-failover-vr) #
```

When a virtual router fails, the associated failover group's `priority` value is decremented by the `priority-delta` value (2) to a new `priority` value and a comparison is done between the priorities of the failover groups on the two chassis. In this example, the `priority` value on Chassis 1 becomes 248, which is less than the `priority` value of the associated failover group on Chassis 2, so the failover group on Chassis 2 becomes the master. The `priority-delta` value is added back to the `priority` when the VR recovers.

3. Specify the MAC usage on the VRRP Virtual Router.

```
CBS(conf-vrrp-failover-vr) # mac-usage vrrp-mac
CBS(conf-vrrp-failover-vr) #
```

When you specify `vrrp-mac` as the MAC usage parameter, instead of using the same MAC address on both the circuit and virtual IP address, XOS automatically generates a unique `vrrp-mac` (for example, `00:00:5e:00:01:10` where the last two digits represent the VRRP ID of the Virtual Router). In the event of a failover, the MAC address moves with the virtual IP address to the new chassis. Keeping the MAC address consistent enables faster convergence and enables stateful VPN failover.

4. Specify the VAP Group of the Virtual Router.

```
CBS(conf-vrrp-failover-vr) # vap-group fw1
CBS(conf-vrrp-vr-vapgroup) #
```

NOTE: The circuit must already be mapped to the VAP group.

Specifying the VAP group of the virtual router allows you to assign a virtual IP address to the VAP group.

5. Assign a virtual IP Address to the Virtual Router, and return to the main CLI context.

```
CBS(conf-vrrp-vr-vapgroup) # virtual-ip 4.0.0.1/24
CBS(conf-vrrp-vr-vapgroup) # end
CBS#
```

NOTE: The maximum number of virtual IP addresses that can be configured on a virtual router is 99.

2.6.4 Enable VRRP on the VAP Group

VRRP monitors the fw1 VAP group for failure of individual VAPs. By setting the `active-vap-threshold` and the `priority-delta`, individual VAP failures can decrement VRRP priority and cause a comparison with the VRRP priority on the remote chassis. Failover occurs when the `priority-delta` value decrements the priority value of the master failover group below the priority value of the associated failover group on the remote chassis. In our configuration, the priority value for the master failover group is 250 and the priority value for the backup group is 249. A `priority-delta` of 2 is used for each of the VAP groups.

To configure the fw1 VAP group for failover:

1. Enable VRRP on the fw1 VAP group.

```
CBS# configure vrrp vap-group fw1
CBS(conf-vrrp-vap-group) #
```

2. Assign the VRRP enabled fw1 VAP group to a failover group list (required).

```
CBS(conf-vrrp-vap-group) # failover-group-list fogrp1 fogrp2
CBS(conf-vrrp-vap-group) #
```

3. Optionally, set the hold down timer.

Configure the `hold-down-timer` to 120, which forces the VAP group to wait for two minutes while the application fully boots. This wait prevents the failover group from becoming VRRP master before the application is fully active.

```
CBS(conf-vrrp-vap-group) # hold-down-timer 120
CBS(conf-vrrp-vap-group) #
```

4. Optionally, set the active VAP threshold and return to the main CLI context.

The `active-vap-threshold` monitors the number of active VAPs in the VAP group. If the number of active VAPs drops below the threshold, the failover group's `priority` value is decremented by the `priority-delta` (defined in Step 5) and a comparison is done between the priorities of the failover groups on the two chassis. Failover occurs when the `priority-delta` decrements the `priority` value of the master failover group below the `priority` value of the backup group.

```
CBS(conf-vrrp vap-group) # active-vap-threshold 3
CBS(conf-vrrp vap-group) # end
CBS#
```

5. Set the `priority-delta` value for the VAP group (optional).

Assign a `priority-delta` to the VAP group. VRRP decrements the `priority` of the failover group whenever the number of active VAPs falls below the `active-vap-threshold`.

The `priority-delta` value can be any number between 1 and 255 and the default value is 1. When the VAP returns to the Active state, the `priority-delta` value is added back to the `priority` value.

```
CBS(conf-vrrp-vap-group) # priority-delta 2
CBS(conf-vrrp-vap-group) # exit
```

2.7 Preemption

Typically, after a failover has occurred from one failover group to another, you want the failover group that is now master to remain in that role, even after the problem that caused the failover has been resolved.

By default, preemption is turned off, and Crossbeam recommends that you do not configure preemption for failover groups.

However, if you want the original failover group to resume the role of master, you can turn preemption on using this command.

```
CBS (conf-vrrp-group) # preemption
```

2.8 Management Circuit

If you intend to run Check Point software on the X-Series chassis, do not configure the X-Series chassis management circuits as part of any failover group. This configuration is poor design and prevents access by the Check Point management station to the management circuit on the chassis on which the backup failover groups reside .

2.9 Verifying Your Configuration

This section contains the output of several commands that show the configured status of Chassis 2. To check your progress throughout the configuration process, open a second CLI window, log in to the CPM and enter one of the commands.

Output of show running-config on Chassis 2

```
CBS# show running-config
#
remote-box 45 1.1.45.20 192.168.50.45 192.168.51.55
#
vap-group fw1 xslinux_v5
  vap-count 3
  max-load-count 3
  ap-list ap1 ap2 ap3 ap4 ap5 ap6 ap7 ap8 ap9 ap10
  load-balance-vap-list 1 2 3 4 5 6 7 8 9 10
  ip-flow-rule loadbalance1
    action load-balance
    activate
#
circuit Gig12 circuit-id 1025
  device-name Gig12
  vap-group fw1
  ip 3.0.0.3/24 3.0.0.255
circuit Gig22 circuit-id 1026
  device-name Gig22
  vap-group fw1
  ip 5.0.0.3/24 5.0.0.255
circuit Gig17 circuit-id 1027
  device-name Gig17
  vap-group fw1
  ip 2.0.0.3/24 2.0.0.255
circuit Gig27 circuit-id 1028
  device-name Gig27
  vap-group fw1
  ip 4.0.0.3/24 4.0.0.255
```

Chapter 3: Active-Active VRRP Dual-Box High Availability Configuration

```
circuit sync circuit-id 1029
  device-name sync
  link-state-resistant
  vap-group fw1
    ip 6.0.0.14/24 6.0.0.255 increment-per-vap 6.0.0.16
#
interface gigabitethernet 1/2
  logical Gig12
  circuit Gig12
interface gigabitethernet 2/2
  logical Gig22
  circuit Gig22
interface gigabitethernet 1/7
  logical Gig17
  circuit Gig17
interface gigabitethernet 2/7
  logical Gig27
  circuit Gig27
#
vrrp failover-group fogrp1 failover-group-id 1
  priority 249
  virtual-router vrrp-id 10 circuit Gig12
    priority-delta 2
  vap-group fw1
    virtual-ip 3.0.0.1/24 3.0.0.255
  virtual-router vrrp-id 11 circuit Gig22
    priority-delta 2
  vap-group fw1
    virtual-ip 5.0.0.1/24 5.0.0.255
vrrp failover-group fogrp2 failover-group-id 2
  priority 250
  virtual-router vrrp-id 20 circuit Gig17
    priority-delta 2
  vap-group fw1
    virtual-ip 2.0.0.1/24 2.0.0.255
  virtual-router vrrp-id 21 circuit Gig27
    priority-delta 2
  vap-group fw1
    virtual-ip 4.0.0.1/24 4.0.0.255
vrrp vap-group fw1
  failover-group-list fogrp1 fogrp2
  hold-down-timer 120
  priority-delta 2
management gigabitethernet 13/1
  ip-addr 192.168.50.45/24 192.168.50.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 13/2
  ip-addr 192.168.51.55/24 192.168.51.255
  enable
  access-list 1 input
  access-list 2 output
```

```

management gigabitethernet 14/1
  ip-addr 192.168.50.65/24 192.168.50.255
  enable
  access-list 1 input
  access-list 2 output
management gigabitethernet 14/2
  ip-addr 192.168.51.75/24 192.168.51.255
  enable
  access-list 1 input
  access-list 2 output

```

Output of show vrrp on Chassis 2

```

CBS# show vrrp
Priority is Actual/Configured
FG-ID  Priority  Status  Preempt  Master Sys ID  Master Priority
1       249/249    Backup  off       45              250
2       250/250    Master  off       46              250
(1 row)

```

Output of show vrrp detail-status on Chassis 2

```

CBS# show vrrp detail-status
FG_ID  Status  Priority  Delta  Type  Component
1  Backup  249/249  2     vr  Gig17/20/0
1  Backup  249/249  2     vr  Gig27/21/0
1  Backup  249/249  2     vg  fw1
2  Master  250/250  2     vr  Gig17/20/5
2  Master  250/250  2     vr  Gig27/21/5
2  Master  250/250  2     vg  fw1

```

NOTE: The Component column shows 5 as the last digit only if you configured the OSPF cost increment as described in [Optionally Configuring OSPF](#) on page 62. If you did not configure the OSPF cost increment, these values would be 0 (zero).

Output of show remote-box on Chassis 2

```

Local System ID: 46
Remote System ID: 45
Remote IP      Local Intf  Local IP      Status  Time In State  Link Qual
192.168.50.45  14/1       192.168.50.46 Active  9 days, 03:10  100
192.168.51.55  14/2       192.168.51.56 Active  9 days, 02:07  100
1.1.45.20      HA port    1.1.46.20     Active  9 days, 02:07  100
(3 rows)

```


Basic Chassis Configuration

This appendix describes the basic configuration of the two chassis. If you have already set up your chassis, you can skip this section and start with [Active-Standby VRRP Dual-Box High Availability Configuration](#) on page 19 or [Active-Active VRRP Dual-Box High Availability Configuration](#) on page 39.

Assign Hostnames

Assign a hostname as follows:

Chassis 1

```
CBS# configure hostname <your hostname goes here> cp1  
CBS# configure hostname <your hostname goes here> cp2
```

NOTE: If you do not specify cp1 or cp2, the hostname is applied to both CPMs.

Chassis 2

```
CBS# configure hostname <your hostname goes here> cp1  
CBS# configure hostname <your hostname goes here> cp2
```

NOTE: If you do not specify cp1 or cp2, the hostname is applied to both CPMs.

Assign a Domain Name

Chassis 1

```
CBS# configure ip domainname <your domain name goes here>
```

Chassis 2

```
CBS# configure ip domainname <your domain name goes here>
```


The following terms are used throughout the Security Services Switch documentation set.

APM

Application Processor Module. The XOS Application Processor system module that provides application processing, status monitoring, and standard and application specific logging. The APM contains one or more CPUs to host applications and network services while processing packets belonging to individual flows.

circuit

An abstract object representing a logical network interface (network service access point). A circuit can be mapped to either single or multiple logical lines. Attributes of a circuit include: a set of physical line or channel pairs, a layer 2 encapsulation type, a layer 2 address, and an IP address (optional).

CLI

Command Line Interface.

CPM

Control Processor Module. The XOS system module that coordinates the actions of all other modules, enables management access to the system, and supports access to a local disk containing configuration files and databases necessary to execute the applications which reside on the platform.

device

OS concept representing either a physical or logical I/O port connected to the APM.

domain

A set of interconnected IP networks belonging to a unique address space. A domain is uniquely identified within the X-Series Platform by a 8-bit domain ID. IP flows must be unique within a given domain.

firewall

A set of software tools that protects a company's internal network from unwanted entry by unauthorized external users. The firewall works in conjunction with a router program to filter incoming network packets and reject those of unknown origin.

flow

Specific stream of data traveling between two endpoints across a network. Specified by source IP, destination IP, source port, destination port and IP protocol type.

flow rule

A filter rule specifying how a packet is processed.

flow specific

A stream of data traveling between two endpoints across a network. Specified by source IP, destination IP, source port, destination port and IP protocol type.

flow table

A table maintained on the NPM that maps individual flows to their respective processors.

IP Address

Internet Protocol (IP). A numerical address that identifies senders and receivers of Internet data. The address accompanies packetized data and identifies it with a particular network on the Internet and the specific device (such as a server) from which it originated.

logical interface

A channelized interface on a physical interface. A subdivision of a physical interface. Currently supported logical interface types are default and VLAN.

logical line

A combination of a physical line and a sub-line (channel). A logical line is uniquely identified by a physical line ID or channel ID pair.

MAC Address

Media Access Control (MAC). A hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub-layers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network media. Consequently, each different type of network media requires a different MAC layer.

NPM

Network Processor Module. The XOS module responsible for network interface access (up to 1 Gbps full-duplex), flow classification, distribution of flows to APMs, and load balancing of the APMs.

physical interface

The physical hardware connector on the NPM or CPM representing a network interface port.

RPM

Red Hat Package Manager.

SCP

Secure copy.

SNMP

Simple Network Management Protocol. The Internet standard protocol developed to manage and monitor nodes on an IP network.

SSH

Secure Shell. A powerful authentication and encryption program replacing older and less secure tools like Telnet. SSH provides both authentication and encryption and is therefore the preferred method of network access. SSH allows a secure connection to be established between a client computer and a server host. The Security Services Switch provides SSH server, SSH client, and scp capability.

VAP

Virtual Application Processor. An application operating environment which can be run on an APM. A VAP consists of the OS, system software, and a set of applications which run concurrently.

VAP group

A virtual set of Application Processor Modules identically configured for load balancing and redundancy to process the same set of applications.

VLAN

Virtual Local Area Network. A local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application).

VND

Virtual Network Device. A Linux kernel object representing a logical network interface. A virtual network device is directly mapped to an NPM circuit.

VPN

Virtual Private Network. Consists of private lines, switching equipment and other networking equipment that are provided for the exclusive use of one customer. A VPN gives users a secure way to access resources over the Internet or other public or private networks using encryption, authentication, and tunneling.

VRRP

Virtual Router Redundancy Protocol. This protocol allows several routers on a multi-access link to utilize the same virtual IP address. One router will be elected as a master with the other routers acting as standbys in case of the failure of the master router. The protocol should also support the ability to load share traffic when both routers are up.

A Virtual Router in XOS is an IP address or a set of IP addresses that can be instantiated on a circuit for a subset of the VAP groups on which the circuit is configured, and active only on one of the X-Series systems participating in multi-system High Availability configuration.

