Blue Coat® Systems

PacketShaper Redundant Setup

Blue Coat®

CONTROL IS YOURS™

Americas:

Blue Coat Systems, Inc.
420 N. Mary Ave.
Sunnyvale, CA 94085

Rest of the World:

Blue Coat Systems International SARL
3a Route des Arsenaux
1700 Fribourg, Switzerland

Document History

Date	Version	Note
January 15, 2013	v0.1	Initial release

Contents

List of Figures

Introduction

High availability is a network topology feature that ensures mission-critical applications are available 100% of the time. This goal is typically accomplished by having multiple access routers with multiple WAN interfaces. PacketShapers can sit in these redundant router topologies and perform their traffic management responsibilities without disrupting the existing high availability configuration. PacketShapers integrate in high availability and redundant environments, including HSRP (Hot Standby Routing Protocol) and VRRP (Virtual Router Redundancy Protocol).

As part of the high availability solution, PacketShapers can be installed in redundant network paths to provide PacketShaper redundancy in case one of the units fails. This capability is called *direct standby*.

Direct standby allows two PacketShapers to work in a redundant network topology, with each unit connected to a different router, and the two units directly connected to each other. Both units are considered active, and each unit can receive and forward traffic. To ensure that both units accumulate the same traffic tree and measurement data, each PacketShaper processes the packets received by the other unit. When a unit directly receives traffic, it will copy that traffic and transmit it to the other unit. The other unit will classify the traffic, just as if it had received it directly, but it will never forward the traffic onward to the LAN. As a result, each unit is ready at any time to take over full PacketShaper responsibilities if the other unit goes down.

Direct standby can operate in a redundant topology that is set up to do load balancing (traffic flowing through both paths) or one that is set up as a backup, in case of component failure (traffic flowing through one path). When using the direct standby feature in a load-sharing topology, you should set the link speed to the sum of both WAN links.

Note: Because each unit receives copied packets from its partner, the PacketShaper must have overall inbound and outbound partition sizes that will support that level of extra traffic.

Requirements

The direct standby feature is *absolutely mandatory* when network traffic is asymmetric, and particularly on a single site where there is risk of crossing a PacketShaper for egress traffic and another PacketShaper for ingress traffic (or vice-versa). PacketShapers are application-aware, so in order to correctly classify applications based on their Layer 7 signature in asymmetric topologies, PacketShaper needs to see both ingress and egress traffic flow. In case direct standby is not activated in these redundant scenarios, PacketShaper will misclassify applications, and TCP Rate Control algorithms will not behave as expected.

Direct standby has the following requirements and limitations:

- The direct standby connection between both PacketShapers *must be* direct (no switching/routing in between). PacketShaper replicates the traffic towards the direct standby peer. Duplicated packets have the wrong CRC checksum that requires a direct connection between PacketShaper (through fiber or copper interfaces). For this particular case, the first thing to know is whether the WAN/Internet routers are located in the same room, or close enough to connect directly to both PacketShapers.
- ATM and Frame Relay features, as well as watch mode, cannot be used in conjunction with the direct standby feature.
- PacketShaper 12000: The units are directly connected using their built-in Standby ports. If you have disabled the built-in Standby port, you can connect the units between the outside interfaces of the right-most pairs on each installed LAN Expansion Module (LEM).
- PacketShaper 3500, 7500, 10000: The units must be directly connected to the outside ports on the upper-most or right-most LEM. In other words, if the PacketShaper has two LEMs, the upper or right LEM must be used for the direct connection. This LEM cannot be configured for Xpress Compression.
- Both units must be running the same version of PacketWise and have the same plugins installed.
- Both units must have the same configuration limits. For example, both units must be 1024-class PacketShaper 3500s. You should not mix units with different capacities, because the units will be passing the same traffic and require identical configurations.
- Both units must have identical hardware configuration: the same PacketShaper model, link speed, installed memory, number of LEMs installed, and type of LEMs (fiber-optic versus copper Ethernet). If there is any difference in the two partner units, the direct standby feature will not function optimally.
- The two units must have the same Touch Password for the direct connection to be established.
- The bypass functionality in the PacketShaper and all LEMs must be disabled in order to use the direct standby feature. If you didn't disable the bypass functionality, enabling the direct standby feature is denied by the PacketShaper.
- Because the bypass functionality has been disabled, PacketShapers should not be powered off when they sit in a redundant configuration. Doing so causes loss of connectivity on that link, and all traffic is routed to the other path.
- The direct link connection between the two PacketShapers must be equal to or greater in speed than each of the WAN links. This requirement ensures that each unit receives copies from the other unit fast enough to prevent out-of-order packets.

- PacketShaper 12000: The total inbound and outbound traffic must be less than approximately 900 Mbps, since the Standby port can handle a maximum of 1 Gbps of traffic. If traffic exceeds 900 Mbps, you may want to use another LEM with 10G capabilities to make sure direct standby operations can work properly.
- A customer portal IP address should not be configured.
- The following types of packets are not copied over the direct connection: broadcast/multicast/unicast packets, and attack packets.
- Link state mirroring (discussed later in this document) is automatically enabled when direct standby is enabled, if the redundant management link is connected.

Scenario

Description

Direct standby allows the PacketShaper to integrate smoothly into a variety of redundant network topologies—those with redundant routers, redundant switches, two data paths, two VLANs, and/or redundant firewalls.

Two PacketShapers each connect to a different router. Both units are considered active, and each unit can receive and forward traffic. To ensure that both units accumulate the same traffic tree and measurement data, each unit processes the packets received by the other. When a unit receives traffic directly, it copies that traffic and transmits it to the other unit. The other unit classifies the traffic, just as if it had received it directly, but does not forward the traffic to the LAN.

Topologies

PacketShapers can be connected into the following types of redundant topologies (not exhaustive):

- Basic failover topology or load-sharing topology (See Figure 1–1.)
- Load-balancing topology (See Figure 1–2.)

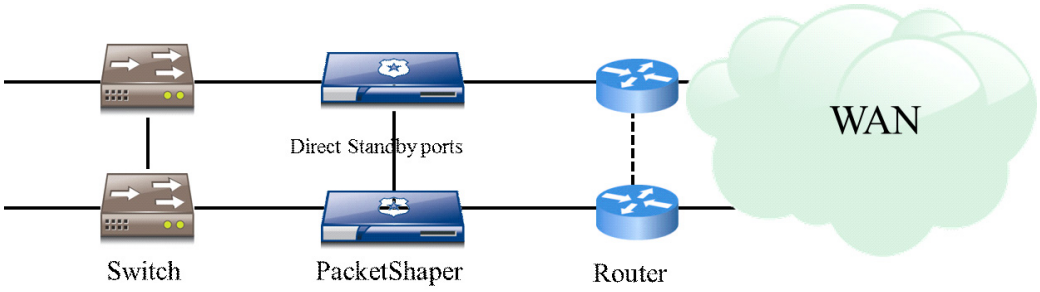

Figure 1–1 Basic failover topology or load sharing topology through Cisco Express Forwarding

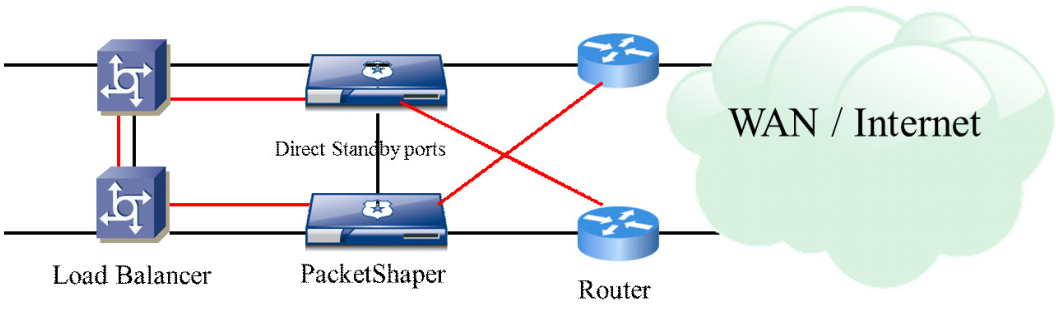

Figure 1–2 Load balancing topology

The method for directly connecting the two units depends on the PacketShaper model:

- PacketShaper 3500, 7500, 10000: Connect the outside ports of the LEMs. If two LEMs are present, you must use the upper-most or right-most LEM for the direct connection between PacketShapers.
- PacketShaper 12000: Connect the Standby ports. If you have disabled the built-in Standby port so that you can use a higher-throughput LEM, connect the outside interfaces of the right-most pair on the installed LEMs.
- PacketShaper 1400: Connect the backup outside ports.

When you connect a PacketShaper in a redundant topology, you can access and manage the unit from any of the LAN-connected ports. If desired, the inside port on the direct standby LEM can be connected to a management network. Note, however, that when this port is connected, it becomes the exclusive management port for the unit; you will not be able to access the unit from the other ports.

Some PacketShaper models have a MGMT port, allowing you a way to connect to a management network. This connection provides a secondary way to access the unit. If you enable the Dedicated Management Port option, you can access the unit through this port only. If both the MGMT port and the inside port on the direct standby LEM are connected, the MGMT port takes precedence.

Configuration Steps

Introduction

Select the topology that corresponds to your network, print the diagram, and follow these instructions.

Procedure:

1. Disable bypass on all interface pairs.
2. On the router, disconnect the straight-through cable that goes to the switch.
3. Reconnect this cable to the PacketShaper's built-in port labeled "inside."
4. Connect the built-in outside port to the router, using the orange crossover cable.

5. Repeat the above steps for the other router/switch.
6. To directly connect the two PacketShapers:
   - PS 12000: Connect a crossover cable between the Standby port on each unit. If you have disabled the built-in Standby port so that you can use a higher-throughput LEM, connect the crossover cable between the outside interfaces of the right-most pairs on each installed LEM.
   - PS 3500, PS 7500, PS 10000: Connect a crossover cable between the outside LEM port on each unit. If a unit has two LEM cards installed, you must use the upper or right LEM.
   - PS 1400: Connect a crossover cable between the backup outside port on each unit.
7. Turn on the PacketShapers.
8. Configure the PacketShapers for direct standby.

Disabling Bypass Functionality

In a default state, the PacketShapers have fail to wire capabilities; however, when dealing with redundant topologies, customers may want to make sure visibility, shaping, and compression can be maintained in case of network problems. Disabling bypass functionality prevents the PacketShaper from allowing flows to pass through to the other network path where the second PacketShaper resides.

In order to enable the direct standby features, you need to disable bypass functionality on all interface pairs. Disabling bypass functionality depends on the PacketShaper models. The PacketShaper 12000 Series has the ability to disable bypass through CLI. For other models, it requires that you power off the unit and remove the jumpers located in the motherboard and LEMs.

On the PacketShaper 12000 Series

Procedure:

1. Access the CLI.
2. For each interface pair (device), use the `setup bypass` CLI command. For example, to disable bypass for all interface pairs:

   ```
   setup bypass open all
   ```
3. Repeat the above steps for the other standby unit.

On other PacketShaper models

Procedure:

1. Power off the unit.
2. Remove power cords, ears, screws, and top cover.

3. Remove nine jumpers from the motherboard. These jumpers are located just behind the inside RJ-45 connector, between two relays, as shown in Figure 1–3.

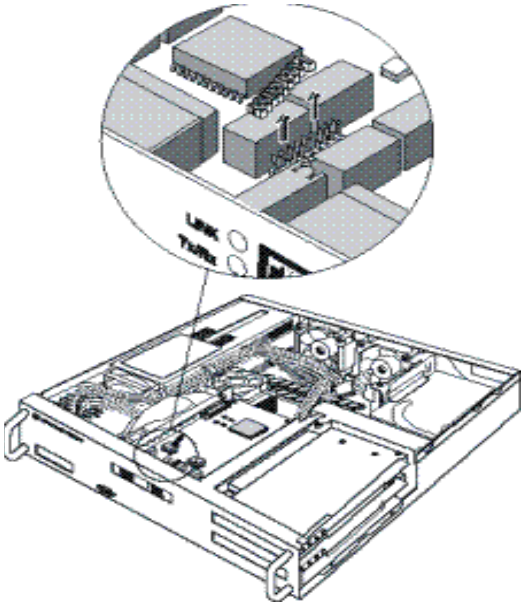

Figure 1–3 Motherboard jumper location

4. Remove the jumpers from all other LEMs (including the direct standby LEM), as shown in Figure 1–4.

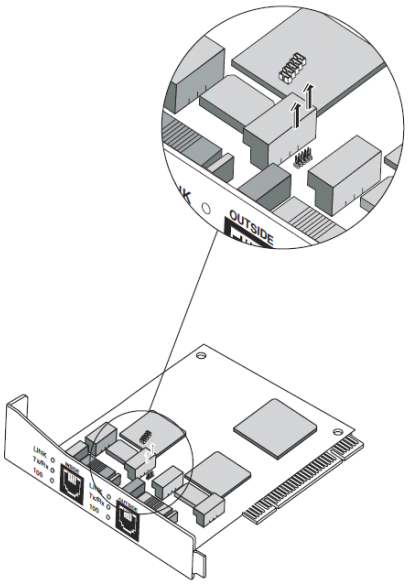

Figure 1–4 LEM jumper location

Note: PacketShapers with fiber-optic connectors do not need to be modified, and the Blue Coat Fiber Bypass Switch should not be deployed.

Configuring PacketShaper for Direct Standby

To configure the PacketShapers for direct standby, complete the following procedure.

Procedure:

1. Configure both PacketShapers with identical passwords. For direct standby to work, both units must be configured with the same Touch Password. (See Figure 1–5.)
   a. On the Legacy user interface, select the **Setup** tab.
   b. Select **Security** from the drop-down list.
   c. Make sure the **Touch Password** is the same on both PacketShapers.

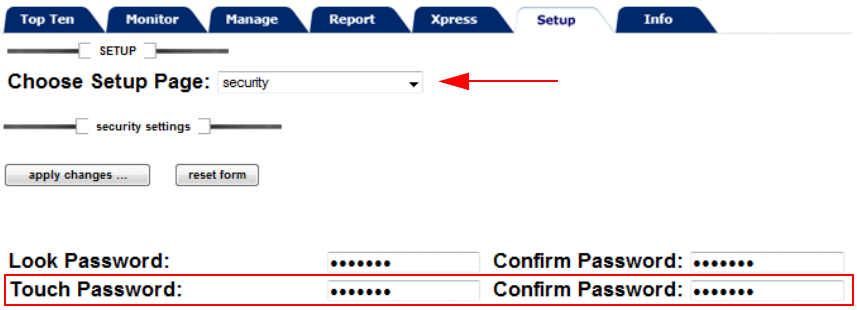

Figure 1–5 Legacy user interface - Setup tab

Note: If you change the password on one of the units when direct standby is enabled, direct standby will continue functioning, giving you an opportunity to change the password on the other unit. However, if one of the units is reset while the two units have different passwords, direct standby is disabled until the passwords are identical and both units are reset (or until standby is turned off and then back on).

2. Make sure both PacketShapers are configured with aggregated bandwidth from all WAN routers. Typically, the inbound and outbound rate should be the sum of all access. This can be done from the **Setup** tab in the Legacy user interface.

   For example, if each PacketShaper is located in front of a WAN router, and each one is handling 10 Mbps symmetric, the inbound and outbound rate must be configured to 20 Mbps on each PacketShaper.

3. Before enabling standby, make sure you have not set the outside interface to secure. (This step is not a requirement for PacketShaper 12000 using the built-in Standby port.) For standby to work, each device must be able to communicate with the other device. If you have set the outside interface to **list**, you must add the partner's IP address to the Outside security list. In the case of direct standby, the unit's own IP address must also be specified on the list. This can be done from the **Setup** tab by selecting **Security** from the drop-down list, then checking the interface security. (See Figure 1–6.)

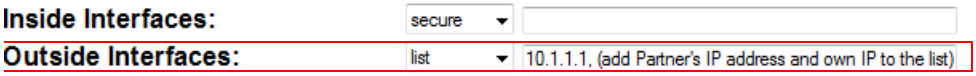

Figure 1–6 Outside Interface set to list

4. When using the direct standby function, the two PacketShapers must have similar traffic trees so that flows are classified and controlled identically, and the same measurement data is collected on each unit. Make sure each unit has the same traffic classes, policies, partitions, and settings.
5. Enable direct standby. (See Figure 1–7.)
   a. Click the **Setup** tab.
   b. Select **standby** from the **Choose Setup Page** drop-down list.

      The **standby configuration** settings display.
   c. Select **Direct** as the standby type.
   d. Click **apply changes**.

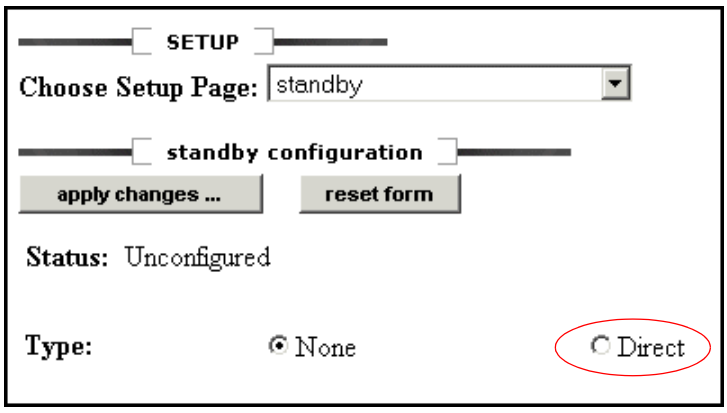

Figure 1–7 Setup page - Direct standby

Note: A loss of connectivity could occur right after direct standby is enabled or disabled. This loss of connectivity is transient and recoverable after the new paths and routes have been established. After the paths and routes have stabilized, you might have to start a new browser session.

Troubleshooting

To verify that direct standby has been configured successfully, you should check the status messages. To access these messages, select the **Setup** tab, then select **standby** from the drop-down list.

For troubleshooting purposes, see Table 1–1 for a list of common status messages.

Table 1–1 Troubleshooting

Status message	Description
Standby/Direct is active with partner <IP@>	The unit has successfully communicated with its direct standby partner. If the unit directly receives traffic, it will copy that traffic and transmit it to the partner unit. The unit will also receive forwarded traffic from the partner; the forwarded traffic will be classified and then dropped.
Standby/Direct has not found a partner.	The unit is unable to establish communication with another PacketShaper. Make sure the units are directly cabled: ❒ PacketShaper 3500, 7500, 10000: though the outside port on the upper-most or right-most LEM ❒ PacketShaper 12000: through the Standby ports ❒ PacketShaper 1400: through the backup outside ports
Standby/Direct disabled (connected to site LAN).	When two PacketShapers are directly connected, traffic is running, and then the direct standby feature is disabled on one of the partner units, the copied packets coming through the direct link between the units are leaking onto the LAN causing the receiving unit to see duplicate packets. Note that this situation happens only for a short time period because the unit sending the copied packets would stop sending packets immediately upon realizing that its partner is down.

Link State Mirroring

When using Link State Mirroring, PacketWise will bring down the second port of a NIC pair if the first port goes down. This feature allows each PacketShaper to sit between a WAN router and a switch without blocking detection of switch outages by the router. Link State Mirroring is automatically enabled when direct standby is enabled and the redundant management link is connected. You can enable/disable Link State Mirroring from the **System Variables** setup page, as shown in Figure 1–8.

To access the **System Variables** setup page, perform the following steps.

1. Click the **Setup** tab.
2. Select **System Variables** from the **Choose Setup Page** drop-down list.

   The **System Variables Configuration** settings display.

3. In the **Miscellaneous** section, select **Yes** from the drop-down list for **Link State Mirroring**. (See Figure 1–8.)

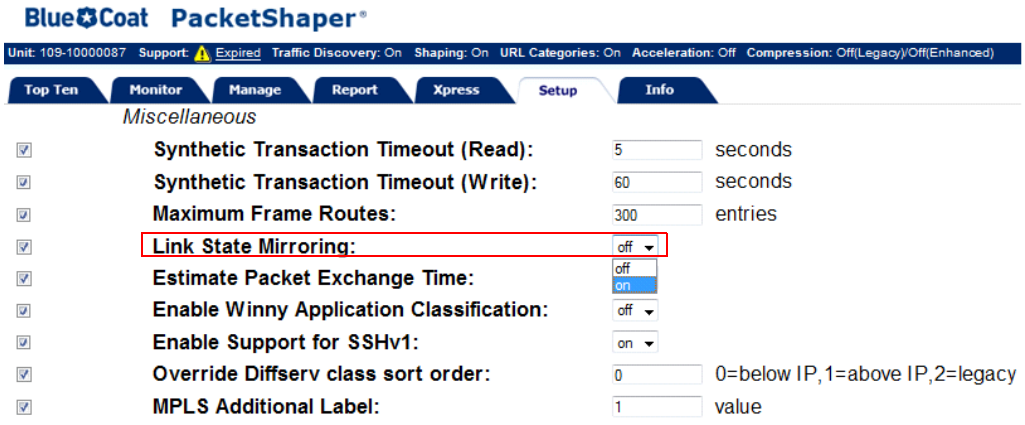

Figure 1–8 System Variables setup page

Note: Link State Mirroring is not active on the LEM being used for the direct link, which allows you to disconnect the redundant management port without impacting connectivity. However, Link State Mirroring is disabled when the redundant management link is disconnected.

Advanced Concepts

PacketShaper Positioning

The direct standby feature is the only way to support PacketShaper redundant topologies when traffic flow is asymmetric. Direct standby ensures that both PacketShapers can have the same vision on network flows, ensuring proper Layer 7 classification.

To ensure proper Quality of Service (QoS) policies, you need to consider the physical topology and how routing is done through customer networks. When a customer has two physical WAN links handling 10 Mbps bandwidth each, you will not manage QoS policies as if it were a single physical access with 20 Mbps.

Even if PacketShaper's QoS policies are enforced dynamically, its configuration (for example, the traffic tree) must reflect the physical topologies and should take routing operations into consideration. Typically, if both WAN accesses are used in an active/active state, either through load balancing or load sharing mechanisms, the traffic tree should take the following into consideration:

- Try to always position the Packetshaper *after* the load balancers. Usually, load balancers have proprietary algorithms to split the load across multiple WAN links. These algorithms are not known by the PacketShaper, so in order to ensure proper QoS, PacketShaper must know which WAN link will be used when packets come through its interfaces. (See Figure 1–9.)

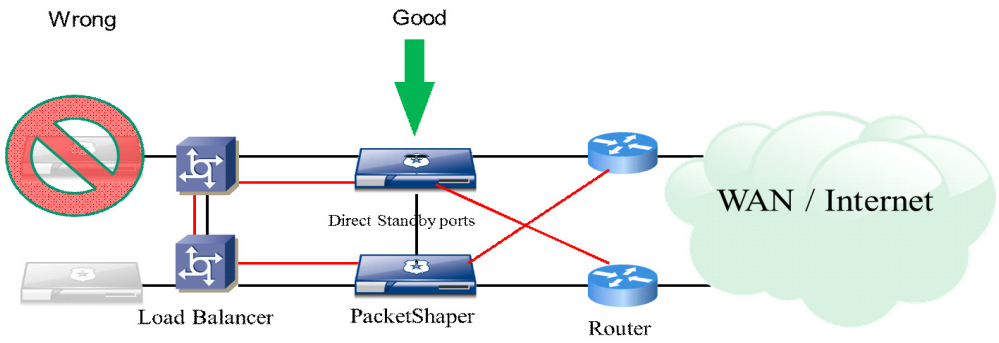

Figure 1–9 Correct positioning of PacketShapers

- When load sharing is configured directly on WAN routers (for example, through Cisco Express Forwarding), make the customer aware that load sharing decisions should ideally be deterministic so that the PacketShaper will know in advance which WAN link will be used to ensure proper Quality of Service.

  Example: The customer should make sure routing decisions are deterministic to ensure proper Quality of Service (QoS). Instead of using dynamic, per-session, load-sharing algorithms, the customer can work with the Service Provider to enhance routing decisions. In that case, in the normal state, remote sites A and B are reachable through WAN Router #1, and sites C and D are reachable through WAN Router #2 in order for the PacketShaper to know in advance as to which WAN link will be used. This allows the customer to manage each WAN link separately, as shown in Figure 1–10.

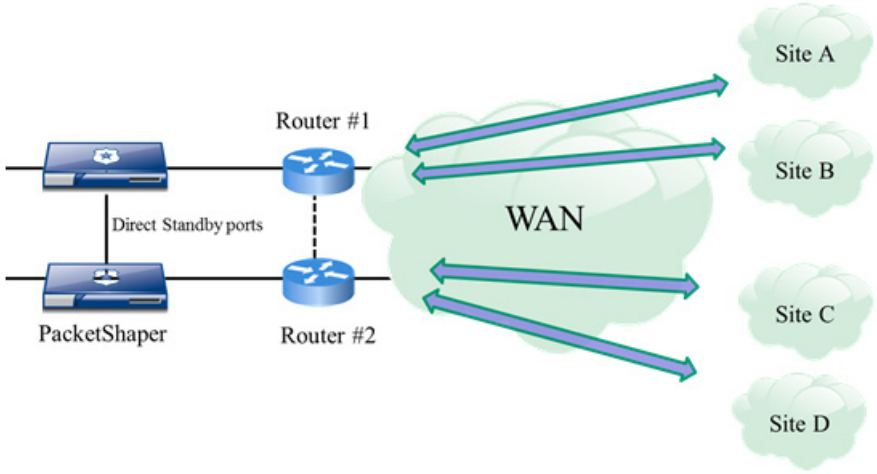

Figure 1–10 Example of deterministic routing with load sharing

Link Failure Detection and Bandwidth Changes

Ideally, the recommended solution should be able to detect problems as they arise. In redundant topologies, if a WAN link goes down, it may impact QoS policies. PacketShapers are individually configured with inbound and outbound rates. As such, when a WAN link goes down, PacketShaper's configurations should reflect the bandwidth changes. This can be done by using one of the following two options:

- "Access Link Monitoring"
- A combination of "Synthetic Transactions and Adaptive Response"

Access Link Monitoring

PacketShaper's Access Link Monitoring feature allows PacketShaper to deal with "imperfect" load-balancing issues and has the ability to respond to the occurrence of WAN link failure. When Access Link Monitoring is enabled, PacketWise can adjust partitions appropriately to prevent overloading any given WAN link and to account for lost available capacity due to router or link failure. Access Link Monitoring has two modes (basic and advanced) and will gather a router's interface status through SNMP. Configuration guidelines and methodologies are beyond the scope of this document, but can be found in the PacketGuide on Blue Touch Online.

Synthetic Transactions and Adaptive Response

The alternative option for detecting a link failure is to use a combination of Synthetic Transactions and Adaptive Response features. In this context, Synthetic Transactions allow the PacketShaper to send traffic (for example, ping, http get) on a regular basis to see if a system is alive. (This can be the Service Provider router, a remote location, a website, etc.) One or more Adaptive Response Agents can then be created to monitor the Synthetic Transaction status.

For example, PacketShaper can send multiple ICMP echo requests every minute to different a remote system. If the location that the PacketShaper is trying to reach is not available, a script is triggered on the PacketShaper to automatically modify its inbound and outbound rates to reflect the WAN link failure. Configuration guidelines and methodologies are beyond the scope of this document, but can be found in the PacketGuide on Blue Touch Online.

Conclusion

The Blue Coat PacketShaper can be deployed in various topologies to provide Layer 7 visibility in the network and enforce QoS policies to prevent business critical applications. This document presents ways to deploy and configure PacketShapers in redundant topologies. It explains the direct standby concepts, requirements, and limitations, as well as advanced concepts, to ensure QoS policies are relevant and consistent across different available network paths.

About Technical Briefs

Technical briefs are designed to illustrate the features and capabilities of Blue Coat products. By describing generic solutions, technical briefs provide a foundation that Blue Coat customers can use to understand how Blue Coat products can be used to solve specific problems.

These technical briefs are not intended to solve customer-specific requests; if you need a customized solution to address a specific concern, contact Blue Coat Professional Services at Professional.Services@bluecoat.com.