SERVICE PROVIDER

Cloud Service Delivery Architecture
Solutions for Service Providers

Technical Paper for Network Engineers

Brocade enables service providers to transition from bandwidth providers to cloud service providers with innovative Virtual Private LAN Services (VPLS)-based cloud service delivery Wide Area Network (WAN) architecture solutions that help them unlock new revenue streams.
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>The Challenge</td>
<td>3</td>
</tr>
<tr>
<td>Brocade Cloud Service Delivery Architecture</td>
<td>4</td>
</tr>
<tr>
<td>Unified Packet Transport</td>
<td>4</td>
</tr>
<tr>
<td>Overview and Benefits</td>
<td>4</td>
</tr>
<tr>
<td>Topologies and Sample Configurations</td>
<td>5</td>
</tr>
<tr>
<td>Multitenancy</td>
<td>5</td>
</tr>
<tr>
<td>Scalability</td>
<td>7</td>
</tr>
<tr>
<td>Endpoint Flexibility</td>
<td>7</td>
</tr>
<tr>
<td>Traffic Load Balancing and Network Resiliency</td>
<td>8</td>
</tr>
<tr>
<td>Hot-Standy Paths</td>
<td>11</td>
</tr>
<tr>
<td>Detour and Bypass FRR</td>
<td>13</td>
</tr>
<tr>
<td>Quality of Service in the Cloud</td>
<td>17</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>19</td>
</tr>
<tr>
<td>Cloud Service Performance, Monitoring, and SLA</td>
<td>21</td>
</tr>
<tr>
<td>Summary</td>
<td>23</td>
</tr>
<tr>
<td>About Brocade</td>
<td>23</td>
</tr>
</tbody>
</table>
INTRODUCTION

Deploying cloud services requires complete consideration of the network within both the cloud data center and the service delivery network (core and metro) connecting the data center to the end users. To ensure optimal application performance and customer experience, service providers must have the ability to provide Service-Level Agreements (SLAs) for all types of services. This paper focuses on the WAN side and details how Brocade® VPLS infrastructure solutions address the challenges faced by service providers and provide a unified network for advanced cloud services.

THE CHALLENGE

The evolution of data consumption and bandwidth needs amplifies pressures on current service provider networks. With the proliferation of smart mobile devices and powerful apps, demand for bandwidth is escalating at a rapid pace. At the same time, increased competition is driving down the price providers can charge for bandwidth services. This leads to a revenue gap that challenges service provider profitability.

Service providers that have their own service delivery network are at an advantage; they can deliver cloud services via their WAN, providing end-to-end service-level guarantees. In addition they can leverage their geographic proximity to the end customer through their Point of Presence/Network Access Points to push content and latency-sensitive application services to the edge of their network, close to the customer. The data center is the new service delivery point, and moving data centers to the service edges helps to reduce backhaul and deliver latency-sensitive, interactive, and location-based services. With a service delivery network and distributed data centers, service providers can alleviate one of their main challenges—significant bandwidth consumption across their network.

Without a reliable and high-performance networking infrastructure to deliver services to end customers, there would be no public cloud service offerings. The unification of the service edge with the data center, the increasing role of virtualization, and the rise of Software-Defined Networking all allow the development of a new flexible and agile framework to deliver services to a provider’s clients. With their data centers and network infrastructure, service providers can deliver end-to-end cloud services with SLAs from access to the data center.
BROCADE CLOUD SERVICE DELIVERY ARCHITECTURE

To satisfy clients’ requirements, cloud providers must have a WAN infrastructure to their data centers that includes a unifying packet transport vehicle that can guarantee cloud Quality of Service (QoS), security, and SLAs, while maintaining high-quality service performance and monitoring. Each of these needs has its challenges.

Within the WAN infrastructure, the primary focus a service provider must have is around unifying packet transport technologies into a single coherent network with consolidated, centralized application management and control. Addressing issues like scalability with technologies like 100 Gigabit Ethernet is a crucial part of this solution as well.

Unified Packet Transport

As service providers move their data centers closer to their customers, the need for scalable, seamless, and unified solutions to interconnect their geographically distributed data centers and deliver services to end users takes on more and more importance. Brocade Multiprotocol Label Switching (MPLS) VPLS is a scalable multitenancy solution targeting data center interconnection and WAN service delivery. Because it is built on top of MPLS, VPLS inherits all the benefits of MPLS, including Traffic Engineering (TE), QoS, Fast Reroute (FRR) and hot-standby Label Switch Paths (LSPs) for quick restoration from any disruptions, and more. VPLS provides fully resilient, multipoint transport of traffic between geographically distributed data centers, allowing for interconnection via one single VPLS domain.

Overview and Benefits

The networking infrastructure requirements for a service provider network to provide VPLS-based data center interconnection services are quite simple. The service provider network should support Provider Edge-to-Provider Edge (PE-to-PE) IP/MPLS. Options for doing so include either Label Distribution Protocol (LDP) or Resource Reservation Protocol (RSVP). To take advantage of the high availability provided by FRR and PE-to-PE traffic load balancing capability utilizing RSVP, Brocade recommends RSVP support in the service provider’s core network. In a Brocade VPLS solution, targeted LDP is used for PE-to-PE signaling. To avoid traffic loops in the service provider network, all the PEs in the same VPLS instance are required to form fully-meshed targeted LDP peering. Traffic received from other PEs is only forwarded to the local customer and never to other PEs. Each VPLS domain is globally identified by a unique Virtual Circuit ID (VC-ID), which should be the same across all PEs. Each PE allocates a label (called the VC label) for each VPLS instance and distributes it to all peered PEs within the same VPLS domain.

Interconnection with customer sites and data centers is simple as well. The Brocade VPLS solution has minimal impact on the existing networking infrastructure for both the service provider and the customer. The customer requires only a single Ethernet port to connect to the cloud service provider, and the provider does not need to overhaul their network to serve a new range of customers. The Brocade interface-based implementation of VPLS Virtual LAN (VLAN) isolates the customer’s VLAN space from the service provider’s VLAN space. In addition to this transparency, the Brocade VPLS solution has the following major advantages for cloud service providers:

- Multitenancy
- Scalability
- Endpoint Flexibility
- Traffic Load Balancing
- Network Resiliency
Topologies and Sample Configurations

Figure 2. An example of VPLS deployment

**Multitenancy**

To support the multitenancy requirements of a cloud environment, the Brocade MPLS VPLS solution provides extensive multitenancy capabilities, with a single Brocade MLXe® supporting 16K MPLS VPLS instances. An individual customer can be served with either single or multiple VPLS instances, depending on its specific requirements. VLAN spaces from different customers are completely isolated from each other in the service provider network, as well as isolated from the service provider itself.

Figure 2 depicts a very basic IP/MPLS network deployment that provides Layer 2 VPLS services to customers. Both Customer A and Customer B are spread across three different physical locations. The same service provider serves both customers and interconnects all their sites together. Customer A has two data centers: one connects to the service provider’s PE3, and the other connects to PE4. Customer A also has a site connecting to PE2, from which some users need to access the two data centers. Customer B’s setup is almost the same, except that one of its data centers is connected to the service provider’s PE1 instead of PE3 like Customer A. VPLS RED is configured for Customer A, while VPLS BLUE is configured for Customer B.

Assume that VLAN 400 is for Customer A and VLAN 500 is for Customer B. The loopback addresses for PE1, PE2, PE3, and PE4 are 10.1.1.1-4/32 respectively. The sample configurations for PE1, PE2, PE3 and PE4 are:
ON PE1:

```
Interface loopback 0
   ip address 10.1.1.1/32
router mpls
   vpls BLUE 200
      vpls-peer 10.1.1.2 10.1.1.4
   vlan 500
      tag interface eth1/1
```

ON PE2:

```
Interface loopback 0
   ip address 10.1.1.2/32
router mpls
   vpls RED 100
      vpls-peer 10.1.1.3 10.1.1.4
   vlan 400
      tag interface eth1/2
   vpls BLUE 200
      vpls-peer 10.1.1.1 10.1.1.4
   vlan 500
      tag interface eth1/1
```

ON PE3:

```
Interface loopback 0
   ip address 10.1.1.3/32
router mpls
   vpls RED 100
      vpls-peer 10.1.1.2 10.1.1.4
   vlan 400
      tag interface eth1/1
```

ON PE4:

```
Interface loopback 0
   ip address 10.1.1.4/32
router mpls
   vpls RED 100
      vpls-peer 10.1.1.2 10.1.1.3
   vlan 400
      tag interface eth1/2
   vpls BLUE 200
      vpls-peer 10.1.1.1 10.1.1.2
   vlan 500
      tag interface eth1/1
```

Configuration 1.


Scalability

In large networks, hundreds of thousands of MAC addresses may have to be maintained, leading to the need for large MAC address tables on each PE device. For even greater scalability, VPLS can be integrated with Provider Backbone Bridging (PBB) at the edge, to provide isolation between customer MAC addresses and provider core MAC addresses. Brocade ensures scalability through the Brocade MLXe Series platform, with support for up to 16K VPLS instances and 1 million MAC addresses.

Endpoint Flexibility

The Brocade MPLS VPLS solution provides flexible endpoint definitions: untagged access endpoints, single .1q tagged endpoints, and dual-tagged endpoints. In the Brocade solution, the proper .1q tag is added or removed from the end user’s traffic before the Ethernet frame is forwarded back to customers, based on the endpoint type configured. The Brocade VPLS implementation also offers VLAN translation functionality. The VLANs for different VPLS endpoints in the same VPLS domain can be different, and VPLS can seamlessly translate the VLAN to match the configuration of local VPLS endpoints. This provides a high degree of flexibility to match different VLAN allocations and configurations across different sites from the same customer.

For example, in the scenario for Configuration 1, you can assume all connections from the service provider to its customers are .1q ports. However, instead of single-tagged interfaces, now assume that Customer A connects to the service provider’s PE3 via an untagged access interface, and Customer B connects to PE1 via a dual-tagged interface with the inner VLAN as 300. Assuming the other configurations stay the same, the configurations on PE1 and PE3 will change to:

ON PE1:

```
Interface loopback 0
    ip address 10.1.1.1/32
router mpls
vpls BLUE 200
    vpls-peer 10.1.1.2 10.1.1.4
    vlan 500 inner-vlan 300
        tagged interface eth1/1
```

ON PE2:

```
Interface loopback 0
    ip address 10.1.1.2/32
router mpls
    vpls RED 100
    vpls-peer 10.1.1.3 10.1.1.4
    vlan 400
        tag interface eth1/2
    vpls BLUE 200
    vpls-peer 10.1.1.1 10.1.1.4
    vlan 500
        tag interface eth1/1
```
ON PE3:

```
interface loopback 0
  ip address 10.1.1.3/32
router mpls
  vpls RED 100
    vpls-peer 10.1.1.2 10.1.1.4
  vlan 400
    untagged interface eth1/1
```

ON PE4:

```
interface loopback 0
  ip address 10.1.1.4/32
router mpls
  vpls RED 100
    vpls-peer 10.1.1.2 10.1.1.3
  vlan 400
    tag interface eth1/2
  vpls BLUE 200
    vpls-peer 10.1.1.1 10.1.1.2
  vlan 500
    tag interface eth1/1
```

Configuration 2.

**Traffic Load Balancing and Network Resiliency**

Brocade VPLS supports load balancing across multiple tunnel LSPs from PE-to-PE. The multiple LSP paths can actively share the traffic carried between the PEs. The LSPs can be configured with primary and hot-standby paths. A failure of the primary path triggers failover to the hot-standby path. Failure detection can be done using RSVP messages. If very fast detection is desired, Bidirectional Failure Detection (BFD) can also be enabled.
To elaborate on Brocade PE-to-PE solutions for VPLS load balancing and tunnel LSP resiliency, Figure 3 continues with the same deployment scenario as Figure 2, with additional details about the service provider network. Four full-meshed P routers are in the service provider core, and each PE router connects to two of the four P routers for physical link redundancy. Each router has a loopback0 interface configured with an IP address 10.1.1.x/32, in which “x” is the router number. For example, PE1’s loopback0 has IP address 10.1.1.1/32, and P5’s loopback0 has 10.1.1.5/32. The links between routers are configured with subnet 10.1.xy/24 respectively, in which “x” and “y” are the router number, with “x” as the smaller of the two. The link between routers PE1 and P5 is configured with subnet 10.1.15/24. Interface e2/1 of PE1 is configured with IP address 10.1.15.1/24, and interface e2/1 of P5 is configured with IP address 10.1.15.5/24. The whole service provider network follows the same rule for IP address configuration.

In order to allow service providers to optimize their networks, Brocade supports multiple methods of VPLS load balancing on PEs. Load balancing can be achieved in two ways: through dynamic load balancing across multiple eligible tunnel LSPs, or by statically specifying a set of tunnel LSPs for a VPLS peer. With the example in Figure 3, assume four tunnel LSPs are configured from PE2 to PE4, and vice versa:

<table>
<thead>
<tr>
<th>From PE2 to PE4</th>
<th>From PE4 to PE2</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP_PE2_P5_P7_PE4</td>
<td>LSP_PE4_P7_P5_PE2</td>
</tr>
<tr>
<td>LSP_PE2_P5_P8_PE4</td>
<td>LSP_PE4_P7_P6_PE2</td>
</tr>
<tr>
<td>LSP_PE2_P6_P7_PE4</td>
<td>LSP_PE4_P8_P5_PE2</td>
</tr>
<tr>
<td>LSP_PE2_P6_P8_PE4</td>
<td>LSP_PE4_P8_P6_PE2</td>
</tr>
</tbody>
</table>
Between PE2 and PE4, both VPLS RED and VPLS BLUE are configured, and there exist four tunnel LSPs in both directions. Traffic between PE2 and PE4 of VPLS RED and BLUE can be configured to dynamically load balance across the four tunnel LSPs. The configurations required for PE4 are:

**On PE4:**

```plaintext
router mpls

path Path_PE4_P7_P5_PE2
    strict 10.1.47.7
    strict 10.1.57.5
    strict 10.1.25.2
    strict 10.1.1.2
    exit

path Path_PE4_P7_P6_PE2
    strict 10.1.47.7
    strict 10.1.67.6
    strict 10.1.26.2
    strict 10.1.1.2
    exit

path Path_PE4_P8_P5_PE2
    strict 10.1.48.8
    strict 10.1.58.5
    strict 10.1.25.2
    strict 10.1.1.2
    exit

path Path_PE4_P8_P6_PE2
    strict 10.1.48.8
    strict 10.1.68.6
    strict 10.1.26.2
    strict 10.1.1.2
    exit

lsp LSP_PE4_P7_P5_PE2
    from 10.1.1.4
    to 10.1.1.2
    primary-path Path_PE4_P7_P5_PE2
    commit

lsp LSP_PE4_P7_P6_PE2
    from 10.1.1.4
    to 10.1.1.2
    primary-path Path_PE4_P7_P6_PE2
    commit

lsp LSP_PE4_P8_P5_PE2
    from 10.1.1.4
    to 10.1.1.2
    primary-path Path_PE4_P8_P5_PE2
    commit
```

The configurations for PE2 are very similar to the configurations for PE4.

Brocade also provides configurable granularity to control which tunnel LSPs can be used to carry PE-to-PE traffic for a specific VPLS instance. In the Configuration 3 example, if the service provider wants to use two out of the four tunnel LSPs between PE2 and PE4 to carry traffic for VPLS RED and the other two for VPLS BLUE, this can easily be achieved by adding the following configurations:

**On PE2:**

```
vpls RED 100
vpls-peer 10.1.1.4 lsp LSP_PE2_P5_P7_PE4 LSP_PE2_P6_P8_PE4
vpls BLUE 200
vpls-peer 10.1.1.4 lsp LSP_PE2_P5_P8_PE4 LSP_PE2_P6_P7_PE4
```

**On PE4:**

```
vpls RED 100
vpls-peer 10.1.1.2 lsp LSP_PE4_P7_P5_PE2 LSP_PE4_P8_P6_PE2
vpls BLUE 200
vpls-peer 10.1.1.2 lsp LSP_PE4_P8_P5_PE2 LSP_PE4_P7_P6_PE2
```

Configuration 4.

In addition to providing the capability to support multiple tunnel LSPs between two VPLS peers for the same VPLS instance, Brocade supports two LSP options to provide flexibility for service providers: hot-standby LSP and FRR-protected LSP for PE-to-PE path failure protection. Both hot-standby LSP and FRR-protected LSP require the RSVP LSPs to be the tunnel LSPs. To provide PE-to-PE network resiliency, either hot-standby LSP or FRR-protected LSP is recommended.

**Hot-Standby Paths**

An RSVP LSP can be configured with one primary path and multiple secondary paths. By default, any secondary path is signaled and established only when the primary path fails. However, to eliminate service outages, this default behavior can be changed by configuring it to signal and establish the secondary path at the same time as the
primary path. When the primary path failure is detected, the already established secondary path takes over within sub-50ms. In such a scenario, the secondary path is operating in hot-standby mode.

LSP with a hot-standby secondary path can be another option that is used in the Configuration 3 example to achieve VPLS PE-to-PE tunnel LSP high availability between PE2 and PE4. Instead of having four LSPs from PE2 to PE4, two RSVP LSPs are configured between each, with a primary path and a hot-standby secondary path. Hot-standby paths can also provide the following advantages simultaneously:

- Concurrent routing and MPLS label switching over the same links
- MPLS LSP signaling protocols: RSVP-TE, LDP
- Traffic Engineering link state database protocols: OSPF-TE, ISIS-TE
- Distribution of IP, L3VPN, and L2VPN traffic across multiple LSPs for load balancing and redundancy
- MPLS over LAG interfaces
- Configurable tunnel experimental bits (EXP) or mapping from customer packet priority
- Priority queuing and scheduling based on EXP at each LSR to ensure service differentiation
- MPLS OAM: LSP Ping and Traceroute
- LSP liveliness monitoring with BFD

Continuing with the example, VPLS RED and VPLS BLUE are both configured to use one of the two LSPs. VPLS RED uses LSP PE2_PE4_RED with primary path Path_PE2_P5_P7_PE4 and secondary path Path_PE2_P6_P8_PE4. VPLS BLUE uses LSP PE2_PE4_BLUE with primary path Path_PE2_P6_P7_PE4 and secondary path Path_PE2_P5_P8_PE4.

**On PE2:**

```plaintext
router mpls
  lsp PE2_PE4_RED
    from 10.1.1.2
to 10.1.1.4
primary-path Path_PE2_P5_P7_PE4
secondary-path Path_PE2_P6_P8_PE4
standby
commit
lsp PE2_PE4_BLUE
from 10.1.1.2
to 10.1.1.4
primary-path Path_PE2_P6_P7_PE4
secondary-path Path_PE2_P5_P8_PE4
standby
commit
vpls RED 100
  vpls-peer 10.1.1.3 10.1.1.4
  vpls-peer 10.1.1.4 load-balance
vpls-peer 10.1.1.4 lsp PE2_PE4_RED
vlan 400
tag interface eth1/2
vpls BLUE 200
vpls-peer 10.1.1.1 10.1.1.4
```
### Configuration 5.

Hot-standby paths are one LSP option for service providers in the Brocade VPLS solution; detour and bypass FRR is another option.

**Detour and Bypass FRR**

Using FRR-protected LSPs is another option for load balancing and network resiliency that Brocade supports. The flagship Brocade MLXe platform provides line-rate label switching of any number of LSPs and numerous optimizations for higher scalability and faster performance, including RSVP Refresh Reduction, Message Bundling, prioritized processing for FRR-protected paths, and CPU offload for BFD, among others.
Unlike RSVP LSP with a hot-standby secondary path to protect the full path, FRR provides more granular control for protecting any segments of an LSP path. FRR on Brocade MPLS provides both one-to-one detour backup and many-to-one bypass facility backup options. When FRR is enabled on an LSP, it defaults to detour backup. If facility backup is desired, you can enable it by entering the “facility-backup” keyword in FRR configuration mode.

Assume, in the Configuration 3 example, that detour backup is desired for tunnel LSPs for both VPLS RED and VPLS BLUE. The necessary configuration to achieve this is:

On PE2:

```plaintext
router mpls
lsp PE2_PE4_RED
  from 10.1.1.2
to 10.1.1.4
  primary-path Path_PE2_P5_P7_PE4
  frr
  commit
lsp PE2_PE4_BLUE
  from 10.1.1.2
to 10.1.1.4
  primary-path Path_PE2_P6_P8_PE4
  frr
  commit
vpls RED 100
  vpls-peer 10.1.1.3 10.1.1.4
  vpls-peer 10.1.1.4 lsp PE2_PE4_RED
  vlan 400
```

Figure 4. Number of LSPs switched to a FRR path.
Configuration 6.

When detour FRR is configured on an LSP, an automatic process is triggered to set up protecting LSP on each node along the LSP path, except for the LSP exiting node, since these are potentially Points of Local Repair (PLR) for the protected LSP. On each potential PLR, a detour path is automatically calculated and signaled with the following priority order:

1. A detour path to next-next-hop along the protected LSP path to protect the link and next node.
2. If the above cannot be set up, fall back to a detour path to next-hop along the protected LSP path to protect the link only.
3. If both of above cannot be set up, fall back to a detour path to next-next-next-hop along the protected LSP until the LSP exiting node is reached.

![Figure 5. Detour FRR-Protected Tunnel LSP.](image-url)
Figure 5 depicts how the tunnel LSP used by VPLS BLUE is protected by detour FRR. The solid blue line is the protected tunnel LSP with path PE2-P6-P8-PE4. The three dotted arrow lines are the detour paths automatically set up by PE2, P6, and P8, which are potential PLR along the protected tunnel LSP path. As the diagram illustrates, PE2 and P6 both set up their detour paths as ending at their next-next-hops (P8 for PE2 and PE4 for P6) along the protected LSP path. P8 sets up its detour path to the next hop, since its next hop is actually the exiting node for the protected LSP.

The configuration for bypass FRR involves a little more manual configuration on potential PLR along the protected LSP path. In the Configuration 6 example, if bypass FRR is desired instead of detour FRR, then in order to achieve the same protection as depicted in Figure 5, the configurations on PE2, P6, and P8 should change to:

**On PE2:**
```
router mpls
  path Path_PE2_P5_P8
  strict 10.1.25.5
  strict 10.1.58.8
  strict 10.1.1.8
  exit
  lsp PE2_PE4_BLUE
    from 10.1.1.2
to 10.1.1.4
primary-path Path_PE2_P6_P8_PE4
frr
  facility-backup
  commit
bypass-lsp BLUE_bypass
  primary-path Path_PE2_P5_P8
  exclude-interface e2/1
vpls BLUE 200
vpls-peer 10.1.1.1 10.1.1.4
  vpls-peer 10.1.1.4 PE2_PE4_BLUE
vlan 500
  tag interface eth1/1
```

**On P6:**
```
router mpls
  path Path_P6_P7_PE4
  strict 10.1.67.7
  strict 10.1.47.4
  strict 10.1.1.4
  exit
  bypass-lsp BLUE_bypass
  primary-path Path_P6_P7_PE4
  exclude-interface e2/5
```
On P8:

```plaintext
router mpls
  path Path_P8_P7_PE4
  strict 10.1.78.7
  strict 10.1.47.4
  strict 10.1.1.4
  exit
  bypass-lsp BLUE_bypass
    primary-path Path_P8_P7_PE4
  exclude-interface e2/1
```

**Configuration 7.**

The exclude interface specifies the protected physical link on PLR, which should not be included in the path of a bypass LSP.

Another benefit of FRR has to do with adaptive LSPs. Brocade has extended FRR protection support to an adaptive LSP, which enables on-the-fly configuration changes on an established LSP. When configuration changes are implemented on an adaptive LSP, the LSP is re-signalized in a make-before-break fashion to avoid traffic disruption. Adaptive LSPs can be enabled simply by adding the keyword "adaptive" to the LSP. For example:

```plaintext
router mpls
  lsp PE2_PE4_RED
    from 10.1.1.2
to 10.1.1.4
  primary-path Path_PE2_P5_P7_PE4
  adaptive
  frr
  commit
```

By supporting both hot-standby paths and detour and bypass FRR, Brocade enables service providers to optimize their networks based on their customers’ needs.

When implementing a cloud service delivery architecture, providers must make sure that the solution not only enacts a unified transport for cloud services, but also addresses considerations like QoS, SLAs, security, and performance and monitoring techniques.

**Quality of Service in the Cloud**

In a service provider cloud network, the capability of supporting end-to-end Quality of Service (QoS) is as important as the capability of differentiating various customers’ traffic and servicing separately. The Brocade QoS implementation provides the capability to honor a customer’s 802.1p Priority Code Point (PCP) setting end-to-end. The PCP value of the incoming customer’s frames can be mapped to MPLS experimental (EXP) bits on the ingress PE, and the MPLS EXP can also be mapped back to the PCP value on the egress PE.

In Brocade QoS architecture, decode-map is used to map packet priority (Differentiated Services Code Point [DSCP], PCP, or EXP) of incoming traffic to an internal priority, while encode-map is used to set the packet priority (DSCP, PCP, or EXP) for outgoing traffic. Customized decode-map and encode-map can be defined globally or on a specific interface if the default map settings are not desired.
For details on Brocade QoS architecture and default map setting, please refer to chapter 14, "Configuring Quality of Service for the Brocade NetIron XMR and Brocade MLX Series," in the Brocade NetIron configuration guide at this link:


Here is a sample configuration to define customized decode-map and encode-map:

Table 1. Decode-map and encode-map customization.

<table>
<thead>
<tr>
<th>Map Type</th>
<th>Sample Configuration</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCP decode-map</td>
<td>qos-mapping</td>
<td>Mapping an incoming frame with PCP 7 to internal priority 3 and drop-prec 2 (optional)</td>
</tr>
<tr>
<td></td>
<td><code>pcp decode-map Customer_decode</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>pcp-value 7 to priority 3 drop-prec 2</code></td>
<td></td>
</tr>
<tr>
<td>PCP encode-map</td>
<td>qos-mapping</td>
<td>Mapping an internal priority 7 and drop-prec 2 to PCP 3 on an outgoing frame</td>
</tr>
<tr>
<td></td>
<td><code>pcp decode-map Customer_encode</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>priority 7 drop-prec 2 to pcp-value 3</code></td>
<td></td>
</tr>
</tbody>
</table>

The decode MPLS VPLS can operate in two different VC modes: tagged mode and raw mode. This gives service providers the flexibility to choose one or the other per VPLS instance, based on a customer’s requirements, enabling service providers to support multiple customer requirements in the same network.

The setting of PCP values of outgoing frames on the egress PE is a little different for the two different modes. VPLS tagged mode enables the preservation of the VLAN tag information in the payload. In VPLS tagged mode, the VLAN priority of the original (incoming) packets is carried across the MPLS cloud to remote peers.

On the ingress PE, the mapping of PCP values to internal priority and MPLS EXP is as follows:

- **Untagged endpoint**: PCP is defaulted to 0 if no other priority setting is in effect (e.g., port priority).
- **Single-/Dual-tagged endpoint**: The PCP of the outer VLAN contributes to the internal priority.
- **The mapping of incoming PCP values to internal priority is controlled by PCP decode-map.**
- **The internal priority is mapped to EXP of the outgoing packets based on EXP encode-map.**

In VPLS tagged mode, the inner VLAN is carried in the payload all the way to the egress PE. The PCP value of the inner VLAN is the same as the one carried in the payload, which is the same as the originally incoming customer’s PCP setting on the ingress PE. On the ingress PE in tagged mode, the PCP value in the MPLS cloud payload is set as the following:

- **Single-tagged endpoint**: the PCP value of the incoming VLAN.
- **Dual-tagged endpoint**: the PCP value of the inner VLAN.
- **Untagged endpoint**: the PCP value is set to 0.

VPLS raw mode behaves differently. By default, VPLS packets are sent to remote peers over the MPLS cloud in raw mode. This means that no VLAN tag information in the payload is carried across the MPLS cloud. On the egress PE in raw mode, the EXP of the VC label are mapped to the PCP values of all VLAN tags (single- or dual-tagged endpoint) for outgoing frames.

In the MPLS cloud, the packets are differentiated and serviced based on different EXP values. On VPLS ingress PE, two labels are pushed on top of the incoming legacy Ethernet frame: an inner VC label and an outer tunnel label. The packet’s priority resides in the EXP field of the MPLS label header. The VC label and the tunnel label carry the same
value in the EXP field. On each LSR, the EXP are propagated according to the EXP decode-map and encode-map settings. The EXP value in the tunnel label controls the QoS behavior on all intermittent LSRs, until the penultimate LSR, on which the tunnel label is popped and the VC label is exposed. The egress PE sees only the VC label, so the EXP value on the VC label is in effect.

On the ingress PE, in addition to mapping the customer’s PCP values on the incoming frame to EXP of the outgoing MPLS packets, Brocade also provides the following options:

- Assign a Class of Service (CoS) value for the VPLS instance at the time of configuration. In this method, the ingress PE router overrides the priority of an incoming frame and selects a tunnel LSP with a CoS value that matches what was configured for the VPLS instance.
- If the incoming frame is untagged, the router can also be configured to assign a priority to the port to determine the CoS value for an incoming untagged Ethernet frame. The priority of a port can be configured from 0 to 7, with a default value of 0.

In an MPLS cloud, transit PE routers and ingress/egress PE routers give an appropriate priority to frames marked with a higher CoS value when making scheduling and congestion-handling decisions. With routers on all segments of service delivery maintaining QoS, customers can be assured that their data and services will be handled properly anywhere in the network.

Cloud Security

As applications, data, and user identity are stretched from a company-specific domain to a provider domain that may be spread out among different organizations in a cloud computing environment, a number of security concerns arise. These issues fall into three broad categories: user authentication policies for customers at the edge, network security policies faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure-as-a-Service via the cloud), and application security and availability.

Brocade provides a comprehensive suite of security solution support, ranging from authentication to network to applications. These include user authentication solutions based on Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), and Secure Shell (SSH). These solutions allow for authentication, authorization, and accounting management for users and computers to connect to and use a network service.

Table 2. Security Policies

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• TACACS+</td>
<td>• MDS authentication</td>
<td>• DDoS mitigation</td>
</tr>
<tr>
<td>• RADIUS</td>
<td>• Password authentication</td>
<td>• SYN attacks</td>
</tr>
<tr>
<td>• SSH</td>
<td>• Flow security policies</td>
<td>• Spam mitigation</td>
</tr>
<tr>
<td></td>
<td>• Access Control Lists</td>
<td>• SSL Certificate Management</td>
</tr>
<tr>
<td></td>
<td>• Virtual Routing and Forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(VRF) tables</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VLANs</td>
<td></td>
</tr>
</tbody>
</table>

There are several types of Distributed Denial of Service (DDoS) attacks, including brute force flooding attacks and protocol-based attacks such as Smurf, ping of death, TCP SYN, and TCP blind reset. See Table 4 for more information.
Table 3. DDoS attacks.

<table>
<thead>
<tr>
<th>Brute Force Flooding Attacks</th>
<th>Protocol-Based Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks are aimed at consuming a finite resource such as CPU bandwidth or a limited amount of buffer space in the system.</td>
<td>Attacks on TCP vulnerabilities include SYN flood, ACK flood, reset attack, and XMAS tree attack.</td>
</tr>
<tr>
<td></td>
<td>Attacks on ICMP include Smurf attack, ping flood, and ping of death.</td>
</tr>
<tr>
<td></td>
<td>Attacks based on fragmentation include teardrop attack and ping of death.</td>
</tr>
<tr>
<td></td>
<td>DNS-based DDoS attacks include DNS amplification attack.</td>
</tr>
</tbody>
</table>

Brocade provides rich solutions to protect against different types of security attacks such as Transmission Control Protocol (TCP)-based attacks (such as TCP SYN) and Internet Control Message Protocol (ICMP)-based attacks (such as Smurf).

To protect against TCP-based attacks, Brocade devices are configurable to drop TCP SYN packets when excessive numbers are encountered. Threshold values can be set for TCP SYN packets that are targeted at the device, which can be dropped when the thresholds are exceeded, as shown in this example:

```
Brocade(config)# ip tcp burst-normal 10 burst-max 100 lockup 300
```

The number of incoming TCP SYN packets per second is measured and compared to the threshold values, as follows:

- If the number of TCP SYN packets exceeds the burst-normal value, the excess TCP SYN packets are dropped.
- If the number of TCP SYN packets exceeds the burst-max value, all TCP SYN packets are dropped for the number of seconds specified by the lockup value. When the lockup period expires, the packet counter is reset and measurement is restarted. In the above example, if the number of TCP SYN packets received per second exceeds 10, the excess packets are dropped. If the number of TCP SYN packets received per second exceeds 100, the device drops all TCP SYN packets for the next 300 seconds.

Brocade also provides enhanced TCP security functionality to protect against other types of TCP-based security attacks, such as TCP blind reset and TCP data injection attacks. This functionality can be enabled by simply adding one line of configuration:

```
Brocade(config)# ip tcp tcp-security
```

In addition to TCP-based attacks, ICMP-based attacks, such as Smurf attacks, are also great threats to cloud security. Brocade products are configurable to protect against Smurf attacks as well:

```
Brocade(config)# no ip directed-broadcast
Brocade(config)# ip icmp burst-normal 5000 burst-max 10000 lockup 300
```

By disabling IP-directed broadcasts, you can avoid being an intermediary in a Smurf attack, while monitoring and limiting ICMP bursts can prevent you from being a victim of such attacks.

Brocade also provides Reverse Path Forwarding (RPF) checks for all traffic that can be enabled either globally or at the interface level. RPF can be configured to reduce IP address spoofing, providing enhanced security for service providers.

With the rich security feature set that is part of Brocade solutions, cloud providers can ease customers’ concerns and protect the sanctity of their data from a wide range of potential security threats.
Cloud Service Performance, Monitoring, and SLA

Cloud service providers need to have fault detection, verification, and isolation of cloud services throughout the network at every level, while simultaneously providing proactive detection of service degradation. OAM tools such as 802.1ag Connectivity Fault Management (CFM) are a standards-based approach to tracking a high level of care for these services. Service fault detection and verification can be achieved through performance monitoring and SLA verification techniques such as Y.1731.

Figure 6. Available OAM tools.

Brocade provides standards-based comprehensive end-to-end OAM tools such as 802.1ag CFM, compliant stack with support for Continuity Check Messages (CCM), LinkTrace, and Loopback messages.

Hierarchical service monitoring for cloud services is supported at every level for both Maintenance Intermediate Point (MIP) and Maintenance End Point (MEP), covering all seven maintenance domain (MD) levels within a maintenance association. These cloud fault detection service supports are available through the entirety of the cloud network, including the customer endpoints and service endpoints with flexible support for Layer 2 VLANs, Layer 3 interfaces, and MPLS endpoints.

Figure 7. Hierarchical service monitoring.
Brocade performance monitoring through Y.1731 allows for real time hardware-based statistics based on Frame Delay and Frame Delay Variation per service, as specified by the maintenance points. The Brocade real-time monitoring technique uses a four-way timestamp mechanism for true roundtrip delay between the cloud customer and the service location within the provider data center.

Figure 7 shows an example of a hierarchical OAM in case MPLS VPLS is configured in the service provider network as the data center interconnection for the customer network. A level 5 MD is configured for customer-to-customer service monitoring, and a level 3 MD is configured for service provider CE-facing PE-to-PE service monitoring. The configurations are:

**On CE1:**
```plaintext
cfm-enable
domain-name customer id 5 level 5
  ma-name ma100 id 100 vlan-id 500 priority 4
  ccm-interval 1-second
  mep 1 down port ethe 1/1
```

**On CE2:**
```plaintext
cfm-enable
domain-name customer id 5 level 5
  ma-name ma100 id 100 vlan-id 500 priority 4
  ccm-interval 1-second
  mep 12 down port ethe 1/1
```

**On PE1:**
```plaintext
cfm-enable
domain-name SP id 4 level 4
  ma-name ma100 id 100 vpls-id 200 priority 4
  ccm-interval 100-ms
  mep 3 up vlan 500 port ethe 1/1
domain-name customer id 5 level 5
  ma-name ma100 id 100 vpls-id 200 priority 4
```

**On PE2:**
```plaintext
cfm-enable
domain-name SP id 4 level 4
  ma-name ma100 id 100 vpls-id 200 priority 4
  ccm-interval 100-ms
  mep 5 up vlan 500 port ethe 1/1
domain-name customer id 5 level 5
  ma-name ma100 id 100 vpls-id 200 priority
```

**Configuration 8.**

A complete WAN cloud service delivery solution offers dependable performance and monitoring techniques, as well as guaranteeing cloud QoS, security, and SLAs. The Brocade VPLS solution provides all this through a unified transport solution that interconnects a provider’s data centers and delivers cloud services to its customers.
SUMMARY

Service providers need a complete cloud solution to combat the revenue gap and network strain that they face today. With Brocade VPLS-based cloud service delivery architecture solutions for their WAN infrastructure, providers can implement a scalable and transparent network with high resiliency and load balancing, enabling providers to differentiate themselves and fortify their position against increased competition.

By virtue of its heritage and technology leadership in both the data center and service provider markets, Brocade is uniquely qualified to help service providers deploy cloud-optimized networks and build out their cloud infrastructures. Brocade VPLS cloud service delivery architecture solutions and Brocade CloudPlex™ with Ethernet Fabrics offer an attractive end-to-end option for service providers to increase scalability, business agility, and resiliency in their network while focusing on cost efficiency as they make the transition from connectivity provider to cloud provider.

See the Brocade NetIron Configuration Guide for more details.

ABOUT BROCADE

Brocade (Nasdaq: BRCD) networking solutions help the world’s leading organizations transition smoothly to a world where applications and information reside anywhere. This vision is realized through the Brocade One™ strategy, which is designed to deliver key business benefits such as unmatched simplicity, non-stop networking, application optimization, and investment protection.

Innovative Ethernet and storage networking solutions for data center, campus, and service provider networks help reduce complexity and cost while enabling virtualization and cloud computing to increase business agility.

To help ensure a complete solution, Brocade partners with world-class IT companies and provides comprehensive education, support, and professional services offerings. (www.brocade.com)