WAN Optimization in MPLS Networks - the Transparency Challenge!

White Paper
Introduction

Today’s modern Wide Area Networks (WANs), such as MPLS networks, provide much more than just a framework for information transport. Many large enterprises use a networking infrastructure provided by a service provider (SP) and employ some or all of its services on the network. In fact, the recent consolidation trend of servers, storage and applications relies more heavily on the WAN to provide an intelligent path for connecting users in remote offices to the core and data center.

Using the provided services, the enterprise can:
- Route traffic (routing/VPN)
- Assure and maintain the network’s connectivity (resilience/Traffic Engineering)
- Prioritize and shape the traffic (QoS/Traffic Engineering)
- Monitor traffic, applications, sessions and users on the network (monitoring)
- Secure traffic (VPN/encryption)
- Protect the network (Firewall/IDS)
- Pay per type of traffic and usage (billing/accounting)

Deploying WAN optimization devices in a modern enterprise WAN can present integration challenges, especially when advanced services such as the ones listed above are used. Most WAN optimization devices tunnel the compressed traffic between appliances, changing the original packet header and payload. Any WAN service that relies on the original packet header information will not be able to function once the header and payload have been hidden inside the tunnel traffic.

Expand Networks’ Accelerator was designed to seamlessly integrate into modern WAN’s through a combination of features and functions.

The Challenges

In order to better understand the integration challenges, let’s look at a real life example:
This enterprise has a central office in New York, three district offices in London, Hong Kong and Johannesburg and about 100 remote branches all over the globe. It uses MPLS infrastructure from the service provider to connect between the offices. Each branch relies on a Customer Edge (CE) router, provided and provisioned by the service provider.

The Customer Edge router is connected to a Provider Edge (PE) router and to the MPLS network core. The Customer Edge router is responsible for routing and preparing (marking) the packet for Provider Edge router labeling inside the MPLS network. The MPLS labeling itself is done in the Provider Edge router.

The Enterprise's IT department uses the following services:

- **QoS:**
  - The MPLS network provides 3 classes of service: Best Effort/Mission Critical/Real-time
  - The Enterprise prioritizes its Citrix/ICA traffic as mission critical, its VoIP as real-time and the rest of the traffic gets best effort
  - The Customer Edge routers implement the necessary classification and marking of the applications

- **Monitoring:**
  - Each Customer Edge router has a NetFlow probe that collects flow information. The center office collects the data and generates reports on traffic flows in the network

- **Security/Protection:**
  - Most of the branches have Firewalls
  - The central office and the district offices have intrusion detection (IDS) appliances
  - The Customer Edge routers provide IPSec encryption for the sensitive data in the organization

Due to slow application response times and high-bandwidth costs, the enterprise decided to deploy Expand Accelerators in most of the branches in order to optimize applications. On average, the Accelerators provided 4 times more bandwidth on the same physical links and optimized response times; however, there were a few potential integration challenges with the current network services in use.

As mentioned earlier, most WAN optimization devices create an IP tunnel to the remote device and send all the compressed packets through this tunnel. The compressed packets have a new IP header that hides the original IP header information. Like all other WAN optimization devices, the Accelerator uses, by default, an IPComp header as the IP header for the tunneled packets. This default encapsulation, however, poses a serious challenge to the additional services used on the network.

As soon as the Accelerator starts to compress traffic, the Customer Edge routers stop seeing the original IP flows and see only IPComp traffic (for compressed traffic). This will cause the following:

- The QoS classification cannot classify Citrix and VoIP traffic and these flows will not be prioritized correctly
- The NetFlow probes will report only on IPComp traffic instead of the original IP flows
Assuming the firewalls and the IDS appliances are deployed after the Accelerator (toward the WAN), they will not be able to protect the sites from internal threats since those threats are tunneled and not visible. The Customer Edge router will not be able to apply encryption on parts of the traffic according to its sensitivity.

Expand is the only vendor to offer an elegant solution to this problem.

The Solution

These integration challenges are common to all the WAN optimization devices available in the market. Expand Networks offers a unique set of solutions that can overcome these integration problems. All of these solutions can be configured easily via the Accelerator’s user-friendly WebUI, or via the Cisco-like CLI.

IP Header Preservation

The Accelerator can be configured to preserve certain fields of the original IP header and copy them to the tunnel’s IPComp header. The Accelerator can preserve the ToS (DSCP) values of the original IP packet and/or the IP source address of the original packet. For some MPLS deployments, preserving these fields is enough to enable the original equipment to tag the packet and prioritize it in the MPLS core.

By default, the Accelerator tunnel’s encapsulation supports IPComp header with ToS preservation.

In our example Enterprise, this mode does not provide sufficient transparency for supporting all the employed services. NetFlow monitoring, for example, will not report on all the IP flows. If the Customer Edge QoS policy is responsible for marking packets, it will not be able to do that in this mode. Also, the security services will not be able to identify threats on the tunneled packets.

Router Transparency Mode

In order to provide full transparency for compressed traffic, Expand Networks offers a unique tunnel encapsulation mode, Router Transparency Mode (RTM). In Router Transparency Mode, the full IP header and the TCP and UDP header are preserved and the network has full visibility of all IP flows.

Using RTM, all of the Enterprise’s current and future services are guaranteed to function properly:
- The Customer Edge routers can classify, shape and mark traffic and IP flows.
- The original provisioning on the routers can be maintained without modification or changes.
- The NetFlow probes can report data on the actual IP flows.
- Encryption can be applied to sensitive traffic.
- Threats (like SYN attacks) can be identified and prevented.
- Unauthorized traffic can be blocked.

In addition, since RTM maintains the original IP flows; it enables the user to employ per-session-services on the network. For example, session-based load balancing and/or session-based QoS schemes.
ToS/ DSCP Marking per Application/ Flow/ Tunnel

In addition to the above capabilities, the Accelerator can assist the Customer Edge routers by performing ToS-bit marking instead of the Customer Edge routers. This can be useful in remote branches that have small, relatively old and/or highly utilized routers. The Accelerator will mark the ToS bits (DSCP) on the original packet and preserve them by using the above capabilities (IP Header Preservation or RTM). The Accelerator can mark packets according to IP sessions, applications or at the tunnel level.

Conclusion

In a modern WAN, full or partial packet transparency is essential for successful integration of different network services that rely on header data. Expand Networks provides a rich set of capabilities that allow the user to deploy Accelerators in complex and feature-rich networking topologies without limiting or disabling additional services that are used in that environment. The most unique offering is Router Transparency Mode. Router Transparency Mode gives the user a best-of-all-worlds solution. This capability enables full integration between Expand Networks’ outstanding compression and acceleration algorithms while guaranteeing compatibility with all current and future advanced WAN technologies.