

# WAN OPTIMIZATION IN MPLS NETWORKS

## 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 can present integration challenges, especially when advanced services such as the ones listed above are used. Most WAN optimization devices tunnel optimized traffic between appliances, changing the original packet header and payload. Any one of the WAN services above that rely 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 transparency features and functions.

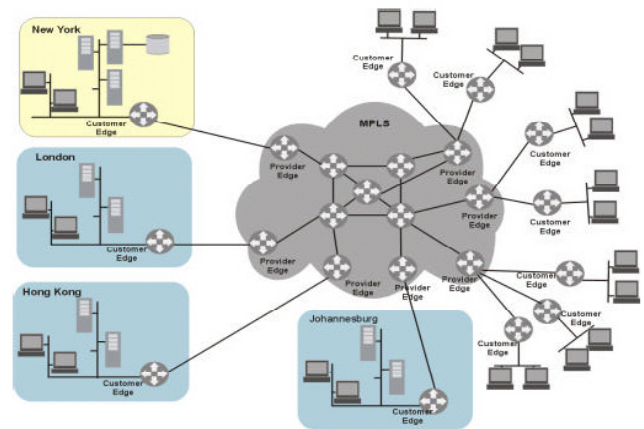
## The Challenges

In order to better understand the integration challenges, let's look at a real life example:

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 the service enabled provider network.

The MPLS labeling itself is done in the provider edge router but requires the identifying marking being completed in order to permit identification.



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:

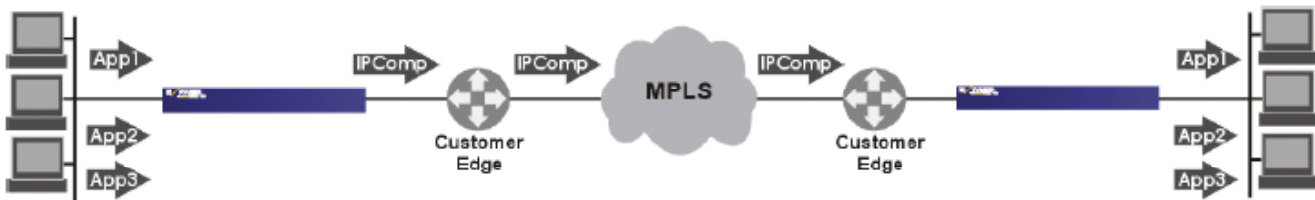
- Most of the branches have Firewalls
- The central office and the district offices have intrusion

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 WAN costs, the enterprise decided to deploy Expand Accelerators to optimize applications, extend control of their network, and condition the WAN for better performance. 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 many 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 – Multiple Layers of Transparency

These integration challenges are common to all the WAN optimization devices available in the market. Expand Networks, however, offers a unique set of solutions that can overcome these integration problems. All of these advanced configuration 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 a IPComp header with ToS preservation. In our example Enterprise, this mode does not provide sufficient transparency for supporting all the employed services. While packets will be routed correctly thanks to ToS preservation, in this case, 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 and may not permit this un-identified but valid traffic to pass.

# WAN OPTIMIZATION IN MPLS NETWORKS



## 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:

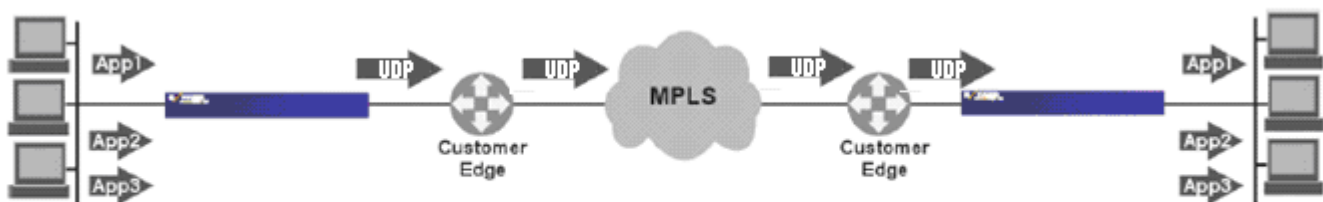
- The Customer Edge routers can classify, shape and mark traffic and IP flows
- The original provisioning on the routers can be maintained without modification or changes
- The NetFlow probes can report data on the actual IP flows
- Encryption can be applied to sensitive traffic
- Threats (like SYN attacks) can be identified and prevented
- Unauthorized traffic can be blocked

Because 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.

In addition to the above capabilities, the Accelerator can assist the customer edge routers by performing ToS-bit marking instead of the edge router. 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.

## Firewall Transparency Mode

Only a secure network is a productive network. Expand encourages the use of intrusion detection, security, and firewalls to protect valuable resources, but these technologies can cripple and disable most WAN optimization solutions as discussed. In these cases more than just header preservation is required for easy implementation of WAN Optimization. Only Expand's Firewall Transparency Mode (FTM) can seamlessly provide security friendly optimized WANs. Similar to Router Transparency Mode, as packets enter the Accelerator they are encapsulated into a fully visible UDP stream. This UDP stream can pass transparently over inspecting firewalls and still enable full firewalling of business critical Wide Area Networks.



Firewall Transparency Mode provides an easy implementation of WAN Optimization on secure networks:

- Completely transparent and compatible to Firewalls and Intrusion Detection systems
- Encapsulates all optimized traffic in efficient UDP flows
- Full featured WAN optimization across deep packet inspected networks.
- Secures networks from malicious use while optimizing business traffic
- Eases implementation, configuration and management on firewalled environments

## 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, secure, and feature-rich networking topologies without limiting or disabling additional services that are used in that environment.

In the industry's most robust and transparent offering, Expand Accelerator's Router and Firewall Transparency Modes give Enterprise the ability to optimize next generation Wide Area Networks. These capabilities enable full integration between Expand Networks' outstanding optimization and acceleration techniques while guaranteeing compatibility with all current and future advanced WAN technologies. Expand can deliver the full power of the industry's best WAN Optimization, granular layer-7 QoS, and virtual branch office services without integration headaches or sacrificing valuable and required WAN based services.