WHITE PAPER

CISCO MULTIPROTOCOL LABEL SWITCHING MANAGEMENT STRATEGY

OVERVIEW

Service providers have adopted different technologies for different applications and services such as voice, video, business-critical data services, and Internet access. Although service providers have been successful in building single-service networks, the current economic and technological needs are positioning Multiprotocol Label Switching (MPLS) as a technology to converge and integrate applications over a single network and to scale existing backbones.

Although MPLS networks are being successfully deployed worldwide, several operational challenges exist in managing, maintaining, and optimizing these deployments. Cisco Systems® is using its internal domain experience, is actively promoting industry standards and their implementation, and is working closely with customers to understand and solve problems related to managing MPLS networks. This solution overview describes Cisco® MPLS network management instrumentation and application capabilities.

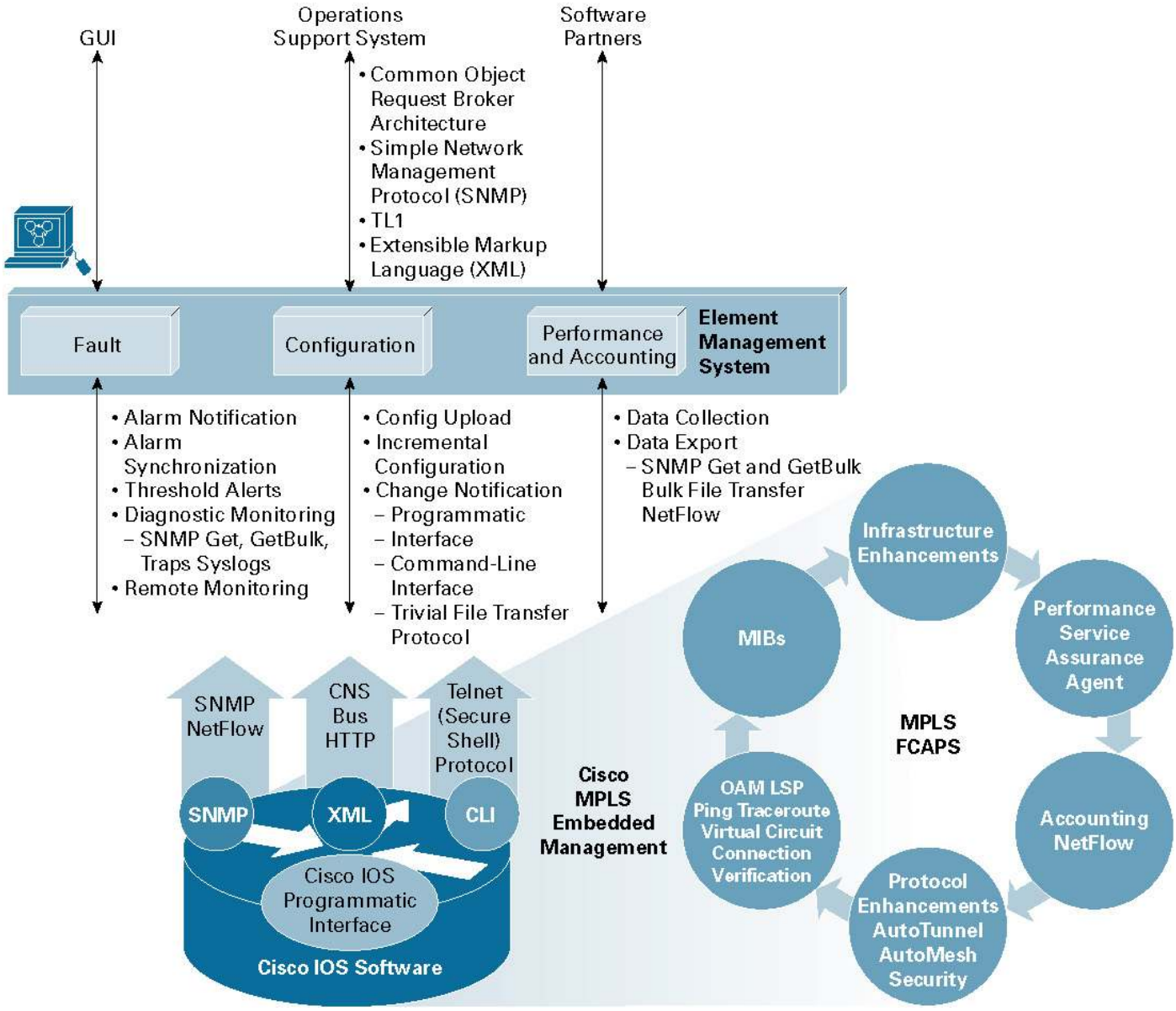
EMBEDDED MANAGEMENT

Most service providers and many enterprises have deployed or have plans to deploy MPLS in their networks. MPLS deployments range from transport applications to customer-specific applications such as voice VPNs (voice over IP over MPLS). As MPLS becomes more mainstream as a converged technology platform, the challenges for optimizing existing assets and investing in next-generation revenue-generating technology has increased. Most MPLS vendor implementations are standards-compliant and hence provide an incentive for large networks to deploy multiple vendors in the network. Having a consistent way of managing and collecting information from the network elements becomes critical to managing fault, configuration, accounting, performance, and security (FCAPS).

Cisco IOS® MPLS Embedded Management offers a set of tools that work together to offer complete MPLS FCAPS. Figure 1 illustrates the Cisco MPLS Embedded Management architecture.

Figure 1

Cisco MPLS Embedded Management Architecture



The building blocks of the Cisco MPLS Embedded Management architecture are described below.

Operation, Administration, and Maintenance Tools

Carriers transitioning from ATM networks to MPLS often expect operation, administration, and maintenance (OAM) applications on MPLS to be similar to ATM OAM applications. Although the problems to be solved on ATM and MPLS networks might be similar, the technology implementations are very different. The main reason for using MPLS OAM, as specified in the document "Detecting MPLS Data Plane Failures" is "When an LSP fails to deliver user traffic, the failure cannot always be detected by the MPLS control plane. There is a need to provide a tool that would enable users to detect such traffic 'black holes' or misrouting within a reasonable period of time; and a mechanism to isolate faults." The following tools address these problems:

- LSP Ping/Traceroute and Pseudo Wire (PWE3) Virtual Circuit Connection Verification (VCCV) use MPLS echo request and reply packets to test label switched paths (LSPs)
- MPLS LSP Ping tests LSP connectivity for IPv4 Label Distribution Protocol (LDP) prefixes, traffic engineering forwarding equivalence classes (FECs) and AToM FECs
- MPLS LSP Traceroute traces the LSPs for IPv4 LDP prefixes and traffic engineering tunnel FECs
- PWE3 VCCV is used to test the pseudo-wire section of an AToM virtual circuit

Performance Tools

The Cisco Service Assurance Agent (SAA) within Cisco IOS Software allows users to monitor network performance between a Cisco router and a remote device (which can be another Cisco router, an IP host, or a multiple virtual storage (MVS) host). Performance can be measured for actual situations through the configuration of Cisco SAA operations that are executed periodically. Various performance metrics measured by Cisco SAA include round-trip response time, connect time, packet loss, application performance, inter-packet delay variance (jitter), and more. This feature allows users to receive notifications, troubleshoot, and analyze problems based on the statistics collected by the Cisco SAA.

With Layer 3 VPN awareness, Cisco SAA allows monitoring within MPLS VPNs. Using Cisco SAA within MPLS VPNs allows service providers to plan, provision, and manage IP VPN services according to customers' service-level agreements (SLAs).

Accounting Tools

MPLS-aware NetFlow is an extension of NetFlow accounting that provides highly granular traffic statistics for Cisco routers. MPLS-aware NetFlow collects statistics on a per-flow basis using the NetFlow Version 9 export format. MPLS-aware NetFlow exports up to three labels of interest from the incoming label stack, the IP address associated with the top label, as well as traditional NetFlow data. A network administrator can turn on MPLS-aware NetFlow inside an MPLS "cloud" on a subset of provider backbone routers. These routers can export MPLS-aware NetFlow data to an external NetFlow collector device for further processing and analysis or show NetFlow cache data on a router terminal. All statistics can be used for detailed MPLS traffic studies and analysis.

The MPLS egress NetFlow accounting feature captures IP flow information for packets undergoing MPLS label disposition; that is, packets that arrive on a router as MPLS are transmitted as IP. One common application of the MPLS egress NetFlow accounting is to capture the MPLS VPN IP flows that are traveling from one site of a VPN to another site of the same VPN through the service provider backbone.

MIBs

MPLS Management Information Base (MIBs) provide open Simple Network Management Protocol (SNMP) interfaces for network operators to rely on vendor element management applications, third-party specialized independent software vendors, or in-house management applications. Some important MPLS MIBs supported in Cisco IOS Software are MPLS-LSR-STD MIB, MPLS-TE-STD MIB, MPLS-FTN-STD MIB, MPLS-LDP-STD MIB, and MPLS-TC-STD MIB.

Protocol Enhancements

Self-configuring and self-healing protocol enhancements help automate provisioning and maintenance of MPLS networks. Cisco IOS Software features such as AutoMesh traffic engineering automatically construct a mesh of traffic engineering LSPs among the provider edge routers. This minimizes the initial configuration of the network and minimizes future configurations resulting from network growth. It also eliminates the need to reconfigure each existing traffic engineering label switch router (LSR) to establish a full mesh of traffic engineering LSPs whenever a new provider edge router is added to the network. Another Cisco IOS Software traffic engineering feature called AutoTunnel Primary and Backup enables a router to dynamically build backup tunnels. This enables a router to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS traffic engineered tunnels.

CISCO MANAGEMENT APPLICATIONS TO SUPPORT MPLS OAM

The Cisco strategy for MPLS management applications is to focus on the delivery of element-layer applications that reduce service provider operating costs for MPLS VPN services. Cisco management applications that support MPLS include:

- Cisco element management systems (EMSs)
- Cisco Info Center
- Cisco Info Center VPN Policy Manager
- Cisco IP Solution Center

Cisco Element Management Systems

Cisco EMSs provide device-level fault, configuration, and troubleshooting capabilities, making use, for example, of MPLS OAM tools such as the MPLS MIBs. Cisco EMSs provide alarm- (trap-) processing capabilities that translate the traps from complex MIB definitions into textual descriptions meaningful to network operations center (NOC) administrators. MIB traps and additional alarm conditions detected by a Cisco EMS can be forwarded to network-layer fault applications, including, for example, the Cisco Info Center, through northbound OSS integration interfaces.

Proactive and detailed device and MPLS troubleshooting tools developed specifically for Cisco routers help ensure that problems can be quickly detected and corrected. Advanced troubleshooting tools allow NOC operators to react quickly to problems and reduce the effects on services running over the network. For a Cisco router in a core MPLS network, GUI-based troubleshooting tools let NOC operators verify ATM as well as MPLS connectivity between routers in the service provider core network or toward the customer sites. In the case of traffic engineered networks, the Cisco EMS includes a single GUI to provide visibility of potential traffic problems within the tunneled network. For example, one issue in a traffic engineered MPLS network could be indicated by the MPLS tunnel operational status being down, indicating a potential problem that can be investigated and rectified.

Troubleshooting tools include:

- Workflow-oriented user interfaces to help solve MPLS forwarding problems
- GUIs to provide visibility of MPLS tunnels and LSPs, both head and transit cases
- Workflow-based approaches for diagnosing virtual routing and forwarding (VRF) problems

The need to reduce operational costs has resulted in the Cisco EMS providing a GUI that is free from complex MIB details so that an operator can spot unlabeled packets. Cisco EMS applications are designed to provide automated troubleshooting capabilities based upon the underlying Cisco IOS MPLS OAM infrastructure. These EMS-based tools support proactive as well as reactive troubleshooting tools and make the Cisco IOS Software capability accessible to more NOC staff members, particularly those who are less experienced. This in turn helps reduce the cost of network operations and reduces time to find faults, increasing customer satisfaction.

MPLS VPN Fault Management and Impact Analysis

An important part of the Cisco MPLS management solution is the umbrella fault management and MPLS VPN impact analysis capability. These functions are offered through the combination of three integrated Cisco products:

- Cisco Info Center
- Cisco IP Solution Center
- Cisco Info Center VPN Policy Manager

Cisco Info Center

The Cisco Info Center provides a customizable, distributed, and integrated client-server system for managing events and alarms from diverse sources, including many different vendor products and standard management platforms. The Cisco Info Center's fault management support includes the use of the Cisco MPLS Embedded Management tool set. The primary purpose of the Cisco Info Center is to consolidate, de-duplicate (suppress repeat events), filter, and correlate fault and alarm information from a wide range of management platforms and products. The Cisco Info Center can receive events from any MPLS-capable device and display those events on the Cisco Info Center desktop. Integration with the Cisco IP Solution Center and Cisco Info Center VPN Policy Manager allows the Cisco Info Center to show the effects of device-specific faults on customers' VPNs, clearly showing which customers are affected by lower-layer device fault conditions. As a result, service providers can meet their SLA commitments to their customers.

Cisco IP Solution Center

The Cisco IP Solution Center is an element Layer 2 and Layer 3 MPLS provisioning application offering support across a wide range of Cisco platforms, from Cisco 3600 Series routers to Cisco 12000 Series routers. The Cisco IP Solution Center manages a range of Layer 2 and Layer 3 MPLS related technologies, including:

- VPNs based on MPLS Border Gateway Protocol (BGP), IP Security (IPSec), AToM, and Frame Relay over MPLS
- Metro Ethernet services such as Ethernet virtual connection services, transparent LAN services, and Ethernet to the home, building, or campus (ETTx)

Cisco Info Center VPN Policy Manager

The Cisco Info Center VPN Policy Manager integrates with Cisco IP Solution Center to enable a deeper understanding of which MPLS VPNs are affected by a network fault, how to prioritize events, and how to effectively and quickly troubleshoot a problem. Once the VPN has been analyzed, a report is sent back to the Cisco Info Center detailing the affected MPLS VPNs and the customers using those VPNs. This information is presented to the NOC or VPN user as a specific Customer Network Managed view.

This capability provides clear benefits:

- Faults are automatically captured and correlated to clearly identify affected MPLS VPNs and customers quickly.
- Troubleshooting tools exploit intelligent Cisco IOS MPLS features such as the Cisco MPLS Embedded Management tool set described above for much faster MPLS troubleshooting.
- A system-based combination of event collection, service-level correlation, and sophisticated troubleshooting tools gives full lifecycle event management and reporting for MPLS networks based on Cisco equipment.

CONCLUSIONS

Cisco provides a comprehensive suite of MPLS management tools and applications from embedded management and instrumentation to element and network management applications. Integrated management gives service providers a system-based approach for minimizing their MPLS OAM costs and the tools they need to support their customer SLAs. Cisco is promoting MPLS OAM standards and mechanisms based on customer requirements for Layer 2 and Layer 3 services deployed over MPLS-based networks. These requirements and mechanisms are evolutionary, as articulated by customers. Cisco customers gain a true competitive advantage and reduce the cost of operations by deploying the Cisco MPLS solution.

REFERENCES

IETF Standards[1]

OAM Requirements for MPLS Networks:

http://www.ietf.org/internet-drafts/draft-ietf-mpls-oam-requirements-02.txt

MPLS LSP Ping/Traceroute:

http://www.ietf.org/internet-drafts/draft-ietf-mpls-lsp-ping-05.txt

LSR Self Test:

http://www.ietf.org/internet-drafts/draft-ietf-mpls-lsr-self-test-02.txt

VCCV:

http://www.ietf.org/internet-drafts/draft-ietf-pwe3-vccv-02.txt

Bidirectional Forwarding Detection:

http://www.ietf.org/internet-drafts/draft-katz-ward-bfd-02.txt

OAM Message Mapping:

http://www.ietf.org/internet-drafts/draft-nadeau-pwe3-oam-msg-map-04.txt

Bidirectional Forwarding Detection MIB:

http://www.ietf.org/internet-drafts/draft-nadeau-bfd-mib-00.txt

[1] Please note IETF references that are Internet drafts are subject to expiration after 6 months. If this occurs please try upping the revision number or searching the IETF drafts database at http://www.ietf.org.

Cisco IOS Software MPLS Embedded Management Tools

MPLS OAM

Cisco MPLS Embedded Management—LSP Ping/Traceroute and PWE3 VCCV:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/gslsppt.htm

Cisco SAA

Cisco SAA Support for MPLS VPN Monitoring:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft1csaa.htm

NetFlow

MPLS-Aware NetFlow:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fsmnf26.htm

MPLS Egress NetFlow:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/egress.htm

Protocol Enhancements (Self-Configuring Tools)

MPLS Traffic Engineering AutoTunnel Mesh Groups:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/gsmeshgr.htm

MPLS Traffic Engineering AutoTunnel Primary and Backup:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s27/gsautotn.htm

Cisco MPLS Embedded Management Applications

Cisco Info Center:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/index.html

Cisco Info Center VPN Policy Manager:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/products_data_sheet09186a00801f5059.html

Cisco IP Solution Center:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/index.html

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

AW/LW5739 0504