Cisco IOS® MPLS Management Technology Overview

Enabling Innovative Services

February 2004
Agenda

• Introduction
  Problems, challenges, requirements

• Technology Overview

• Summary
Service Provider Problems

• **Operational Efficiencies**
  Increase management automation and availability

• **New Services Provisioning**
  Enable competitive differentiation and customer retention through profitable bundled services

• **Disparate Networks**
  Manage and consolidate traditional and emerging networks
MPLS Service Provisioning Challenge

Challenges in VPN Service Provisioning

- Integration with OSS and Billing System: 65%
- Number of Network Elements Involved: 47%
- Integrating Multiple Technologies into a Single Service: 47%
- Finding Customer Self-Provisioning Tools that Work: 41%
- Equipment Manufacturer Management System Not Designed for Provisioning: 41%
- Interoperability Among Products: 35%
- Manual Configuration of Equipment: 18%

Source: Infonetics, 2003
Reducing OpEx with Network Management

- CapEx typically follows the economy
- OpEx is consistent

Typical ratio of a Tier 1 carrier CapEx vs OpEx spending
- OpEx efficiencies have higher profitability and a higher ARPU

Source: Frost and Sullivan, 2002
Customer Requirements

• Provide systemic management solutions for achieving dramatic productivity gains through automation, intelligence, and simplification

• Enable competitive differentiation and customer retention through high-margin, bundled services
  - Provide automated embedded tools
  - Configuration
  - Error detection & recovery
  - Performance and accounting

• Perform data plane validation with respect to control plane
  - Data plane liveliness and troubleshooting

• Standards and open interfaces, APIs to management/OSS applications and third-party software vendors

• End-to-end circuit/service-level health/alarm correlation
Agenda

• Introduction
• Technology Overview
• Summary
MPLS Management Life Cycle

Cisco Info Center
- Info Server
  - Process Network Alarms
- VPN Policy Manager
  - Determine Service Impact

CISCO IP Solution Center
- OSS
  - Fault
  - Performance Accounting
  - NetFlow Collector

Cisco® IP Solution Center
- EMS
  - Device/Network Provisioning

CNS Performance Engine
- ISV Partners
  - Performance Accounting

MPLS OAM
- LSP created by LDP and/or RSVP-TE
- PWE3 or VPN Label
- Attachment VC OAM's
  - CE
  - Ingress PE
  - Egress PE
MPLS Management Architecture

Fault
- Alarm Notification
- Alarm Synchronisation
- Threshold Alerts
- Diagnostic Monitoring
  - SNMP Get, getBulk, Traps
  - Syslogs
- RMON

Configuration
- Config Upload
- Incremental Configuration
- Change Notification
  - Programmatic Interface
  - CLI
  - TFTP

Performance & Accounting
- Data Collection
- Data Export
  - SNMP Get and GetBulk
  - Bulk file transfer
  - Netflow

Element Management System

Cisco IOS Software

Operations Support System (OSS)
- CORBA
- SNMP
- TL1
- XML

Software Partners

GUI

MPLS FCAPS
- Infrastructure Enhancements
- Performance SAA
- Accounting NetFlow

MPLS Embedded Management
- MIBs
- LSP Ping
- Traceroute
- VCCV
- Protocol Enhancements
  - AutoTunnel
  - AutoMEsh
  - Security

GUI

SNMP

XML

Telnet

SSH

CNS Bus

HTTP

SNMP NetFlow

Cisco IOS Programmatic Interface

CLI

NetFlow

SNMP

Get

getBulk

Traps

Syslogs

Telnet SSH

XML

Cisco IOS Software
## MPLS LSP Ping/Traceroute

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Solution</th>
<th>Applications</th>
<th>IETF Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Detect MPLS traffic black holes or misrouting</td>
<td>• MPLS LSP Ping (ICMP) for connectivity checks</td>
<td>• IPv4 LDP prefix</td>
<td>• Draft-ietf-mpls-lsp-ping-xx.txt</td>
</tr>
<tr>
<td>• Isolate MPLS faults</td>
<td>• MPLS LSP Traceroute for hop-by-hop fault localization</td>
<td>• TE tunnel</td>
<td></td>
</tr>
<tr>
<td>• Verify data plane against the control plane</td>
<td>• MPLS LSP Traceroute for path tracing</td>
<td>• MPLS PE, P connectivity for MPLS transport, MPLS VPN, MPLS TE applications</td>
<td></td>
</tr>
<tr>
<td>• Detect MTU of MPLS LSP paths</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
LSP Ping/Traceroute Example

Ping

MPLS Echo Request

Originating router

Target router

MPLS Echo Reply

TTL=1

TTL=2

TTL=3

Traceroute

Ping Traceroute
# MPLS AToM Virtual Circuit Connection Verification (VCCV)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Solution</th>
<th>Applications</th>
<th>IETF Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ability to provide end-to-end fault detection and diagnostics for an emulated pseudowire service</td>
<td>• AToM VCCV allows sending control packets in band of an AToM pseudowire. Two components:</td>
<td>• Layer 2 transport over MPLS</td>
<td>• Draft-ietf-pwe3-vccv-xx.txt</td>
</tr>
<tr>
<td>One tunnel can serve many pseudowires. MPLS LSP ping is sufficient to monitor the PSN tunnel (PE-PE connectivity), but not VCs inside of tunnel</td>
<td>Signaled component to communicate VCCV capabilities as part of VC label</td>
<td>FRoMPLS, ATMoMPLS, EoMPLS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switching component to cause the AToM VC payload to be treated as a control packet</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type 1: uses Protocol ID of AToM Control word</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type 2: use MPLS router alert label</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VCCV Example

[Diagram showing attachment VCs, LSP pseudowire, LSP tunnel, and ping connections.]
MPLS Traffic Engineering: AutoTunnel – Primary, Backup, & Mesh Groups

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Solution</th>
<th>Applications</th>
<th>IETF Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ability to protect links</td>
<td>• Backup AutoTunnel—Enables a router to dynamically build backup tunnels</td>
<td>• MPLS VPN with multiservice SLAs (voice, video, and data sites)</td>
<td>• draft-ietf-mpls-rsvp-lsp-fastreroute-03.txt</td>
</tr>
<tr>
<td>and nodes with no requirement</td>
<td>• Primary one-hop AutoTunnel—Enables a router to dynamically create one-hop primary</td>
<td>• MPLS AToM-based Layer 2 services with “Bandwidth Assurances”</td>
<td>• draft-ietf-ospf-cap-01.txt</td>
</tr>
<tr>
<td>of “traffic engineering”</td>
<td>tunnels on all interfaces that have been enabled with MPLS TE tunnels</td>
<td>• Enhanced SLA service offerings with low packet loss during failure condition – “Bandwidth</td>
<td>• draft-vasseur-mpls-ospf-te-cap-xx.txt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protection”</td>
<td></td>
</tr>
<tr>
<td>• Need to ease configuration</td>
<td>• Mesh Group AutoTunnel – Enables automatic establishment of full- or partial-mesh of TE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MPLS Traffic Engineering
AutoTunnel – Primary & Backup

Router A establishes AutoTunnels to adjacent routers –
“automates” configuration of Link & Node Protection

Router configured with AutoTunnel Primary & Backup

Backup AutoTunnel – Next Hop – “Link Protection”

AutoTunnel Backup Next Hop – “Node Protection”

Manually configured Tunnels take precedence over AutoTunnels –
provides “tweaking” capability for customers
MPLS Traffic Engineering
AutoTunnel – Mesh Groups

Routers A, B, C, D, E – defined as members of “Mesh Group 1”
Capable of building multiple meshes for DiffServ aware Traffic Engineering
Automates configuration of full mesh of TE Tunnels resulting in operational efficiencies
# MPLS-Aware SAA

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• IP SLA monitoring for MPLS VPNs</td>
</tr>
<tr>
<td></td>
<td>• Network performance monitoring per VPN</td>
</tr>
<tr>
<td></td>
<td>• Hop-by-hop statistics for troubleshooting</td>
</tr>
<tr>
<td></td>
<td>• Low-cost solution embedded in Cisco IOS® Software</td>
</tr>
<tr>
<td></td>
<td>• Active traffic generation within Cisco IOS using SAA</td>
</tr>
<tr>
<td></td>
<td>• Jitter, packet loss, latency, connectivity</td>
</tr>
<tr>
<td></td>
<td>• CPE to CPE, PE to CE, and PE to PE measurements</td>
</tr>
<tr>
<td></td>
<td>• SAA PE, multi-vrf CE or dedicated SAA router</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applications</th>
<th>IETF Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>• MPLS, MPLS-VPN, MPLS-TE</td>
<td>• RFC 1889 Jitter Compliant metrics</td>
</tr>
</tbody>
</table>
SAA VPN Measurements

Per VPN Performance Monitoring
Packet loss, Latency, Jitter, Connectivity
• PE to PE, CE to CE, PE to CE, PE to remote CE

Cisco IP Solution Center
Cisco® Info Center
Partner Reporting Applications

CNS Performance Engine 2.1

SAA MIB Data

Blue VPN site 1
SAA
CE

Blue VPN site 2
SAA
CE

Blue VPN site 3
SAA
CE

Red VPN site 1
SAA
CE

Red VPN site 2
SAA
CE

Dedicated SAA Router

Blue VPN SAA Measurements

© 2004 Cisco Systems, Inc. All rights reserved.
# MPLS-Aware NetFlow

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• MPLS network</td>
<td>• Cisco IOS MPLS-Aware NetFlow</td>
</tr>
<tr>
<td>capacity planning</td>
<td>NetFlow version 9</td>
</tr>
<tr>
<td>• PE to PE traffic matrix</td>
<td>Label export with destination prefix</td>
</tr>
<tr>
<td>• Per-VPN MPLS accounting</td>
<td>Per Label accounting aggregation</td>
</tr>
<tr>
<td>• IP flow analysis</td>
<td>• CNS NetFlow Collector 5.0</td>
</tr>
<tr>
<td></td>
<td>Support of EXP bits as a field to key flow reports on</td>
</tr>
<tr>
<td></td>
<td>Using NFC 5.0 + add on PE-PE Traffic matrix module provides PE-PE traffic matrix aggregation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applications</th>
<th>• MPLS, MPLS-VPN, MPLS-TE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IETF Standards</th>
<th>• IPFIX WG proposed standard</th>
</tr>
</thead>
</table>
MPLS-Aware NetFlow

- Exports up to three MPLS labels, and IP packet information
- Ideal for Traffic Engineering and capacity planning

MPLS-Aware NetFlow (version 9)

Performance Data via FTP

XML Config control

NetFlow Data

CNS Publish and Subscribe Bus

Aggreg. Netflow Data

PerfE: NFC VPN Accounting Module (PE-PE)

CNS FCAPS

NetFlow Collector (NFC)

Third-Party NetFlow Collector

Partner Reporting Applications

MPLS-Aware NetFlow for IP to MPLS traffic

Traditional NetFlow for IP to MPLS traffic

Traffic Flow

Egress MPLS NetFlow Accounting for MPLS to IP traffic

MIB data

SAA MIB data

MPLS

PE

IP

© 2004 Cisco Systems, Inc. All rights reserved.
# MPLS MIBs

| Requirement | • Standards-based SNMP implementation  
| • Integration with existing OSS and third-party vendors/software |
| Solution | • MIBs: LDP, LSR-MIB, TE-MIB, PPVPN-MPLS-VPN-MIB, PWE3-MPLS-MIB, MPLS-FRR-MIB |
| Applications | • MPLS, MPLS-VPN, MPLS-TE |
Cisco Info Center: VPN Policy Manager 3.1

- Cisco Info Center VPN Policy Manager (Cisco Info Center and IP Solution Center integration) correlates network events to affected services
  - CIC VPN Policy Manager available today
- Cisco Info Center VPN Policy Manager 3.1 offers:
  - New Cisco Info Center VPN Policy Manager DSA developed
  - New Cisco Info Center VPN Policy Manager policies developed
  - Device/Interface/Sub-interface MPLS VPN subscriber correlation
  - MPLS troubleshooting tools
Agenda

- Introduction
- Technology Overview
- Summary
Summary

• Provide systemic, integrated, and innovative manageability solutions
• Standards-based open interfaces for easier and faster integration
• Complete end-to-end MPLS service and network management solutions
Cisco leads in the MPLS Market

<table>
<thead>
<tr>
<th>Americas</th>
<th>EMEA</th>
<th>AsiaPac/Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over 200 Customers (MPLS Core &amp; L2/L3 Edge)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cisco IOS MPLS

Smarter
The foundation for more services and more revenues

Enabling Innovative Services

Faster
A flexible QoS framework to enable migration to a converged infrastructure

Lasting
Extensibility to different transports with standards-based open architecture for investment protection